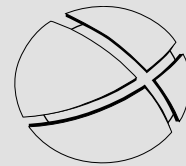


Xincom

TWIN WAN VPN GATEWAY

User Guide

CUTTING EDGE INNOVATIONS.



Model XC-DPG503



XC-DPG503

Twin WAN VPN Gateway

Table of Contents

Introduction	4
Features	5
Physical Details	7
Basic Setup	9
Configuring your LAN	10
Connecting Broadband Modems	12
Configuring for Internet Access	13
Configuring your LAN PCs	14
Advanced Port	16
Port Options	17
Load Balance	18
Advanced PPPoE	19
Advanced PPTP	20
Advanced Setup	21
Host IP Setup	22
Virtual Server	23
Custom Virtual Server	24
Special Applications	25
Dynamic DNS	26
Multi DMZ	27
UPnP	27
Advanced Features	28
Security Management	30
Block URL	31
Access Filter	31
Session Limit	32
Firewall Exception	32

Table of Contents

QoS Configuration	33
VPN Configuration	34
IPSec Global Setting	35
Policy Setup	36
Management Assistant	38
SNMP	38
Email Alert	38
Syslog	39
Upgrade Firmware	40
Operation & Status	42
System Status	42
Restore Factory Defaults	43
WAN Status	43
LAN Status	43
Advanced LAN Configuration	44
Existing DHCP Server	44
Static Routing	45
Appendices	47
Appendix A	47
Appendix B	48
Appendix C	51



Chapter 1 - Introduction

XC-DPG503 Twin WAN VPN Gateway

Chapter Contents

- Introduction
- Features
- Physical Details

XiNCOM XC-DPG503 is a VPN capable Dual WAN Gateway with the industry standard IPsec encryption. It provides extremely secure LAN-to-LAN connectivity over the Internet. The 503 supports VPN by encryption, encapsulation, and authentication using the following methods: DES/3DES/AES, MD5, SHA-1 and SHA-2; up to 50 IPsec tunnels are permitted.

○ **Use TWO ISPs for expanded bandwidth and redundancy**

Using two separate ISPs provides redundant connectivity to the Internet. In the event that one ISP goes down, the XC-DPG503 auto-fails over to the other ISP service. Redundancy to the Internet provides a truly uninterrupted connection for a business's customers while maintaining uptime and productivity for its employees.

○ **Robust Security Features**

The XC-DPG503 also features NAT, a Stateful Packet Inspection (SPI) Firewall, DHCP server, Access Filters, and VPN pass-through to secure a business's network services. The Quality of Service (QoS) feature schedules and directs a network's traffic to take advantage of available bandwidth. The XC-DPG503 UPnP support can dynamically open and close ports required by certain software automatically. Increased bandwidth and redundant connectivity to the Internet provides cost-effective bandwidth solutions to expensive leased telecommunication lines for your network infrastructure.

○ **Package Contents**

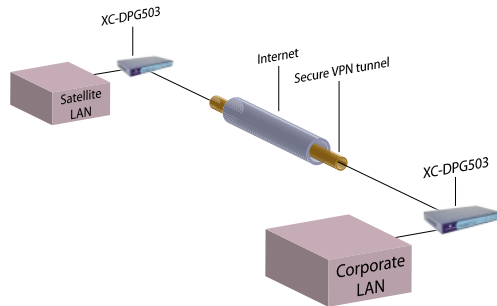
The following items should be included:

- XC-DPG503 Twin WAN VPN Gateway
- Power Adapter (5V)
- Quick Installation Guide
- CD-ROM containing the on-line manual.
- Two CAT RJ-45 Ethernet Cables

If any of the above items are damaged or missing, please contact your dealer immediately.

Features

Figure 1. How it works



Solid VPN Security

Full VPN Endpoint with support for up to 50 VPN tunnels using the IPsec encryption protocol.

Figure 2. Load Balancing

Load Balance two concurrent broadband connections in any combination to expand a network's bandwidth to the Internet. The XC-DPG503 supports T1, xDSL, Cable, and Satellite broadband connections.

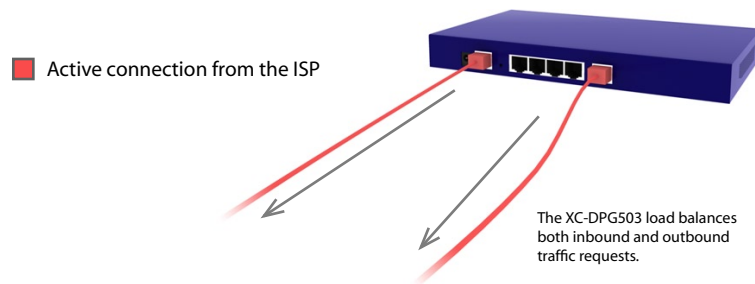
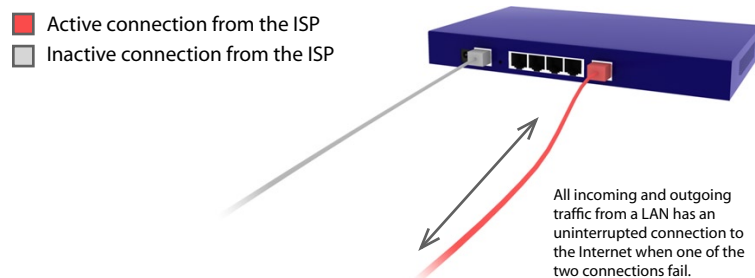


Figure 3. Automatic Fail-over

In the event of one connection going down, all traffic is re-routed to the second WAN port utilizing the live broadband connection from the second ISP. This provides true redundancy to ensure a network remains connected to the Internet.



Built-in VPN Endpoint

Full VPN Endpoint with support for up to 50 VPN tunnels using the IPsec encryption protocol.

Multiple Connection Methods

All popular DSL and Cable Modems and connection methods are supported, including Fixed IP, Dynamic IP, PPPoE, even multiple-session PPPoE.

2 x 10/100 WAN Ports

The XC-DPG503 incorporates dual 10/100 WAN ports, complete with auto-crossover for easy connection to an existing network. All popular DSL and Cable Modems and connection methods are supported, including Fixed IP, Dynamic IP, PPPoE, even multiple-session PPPoE.

4-Port 10/100 Switch

The XC-DPG503 incorporates a 4-port 10/100 N-Way Ethernet Switch, complete with auto crossover for easy connection to an existing network.

Automatic Fail-over

If one broadband connection goes down all traffic is automatically re-routed through the second broadband connection.

Stateful Packet Inspection (SPI) Firewall

Protects your network using advanced SPI against malicious and DDoS attacks.

Advanced NAT features

Access Filters, DMZ, DDNS, Remote Management, Dynamic or Static Routing, Special Applications, Virtual Servers, SNMPv1.

Access Filter

Gain fine control over the Internet access and applications available to LAN users with a powerful URL Blocking Engine. Five (5) user groups are available, and each group can have different access rights.

Block URL

Use this feature to block access to undesirable Web sites by LAN users. You can even have different settings for different groups of PCs.

Features

Other Features:

DHCP Server Support

Dynamic Host Configuration Protocol provides a dynamic IP address to PCs and other devices upon request. The XC-DPG503 can act as a DHCP Server for devices on your local LAN.

Multi Segment LAN Support

LANs containing one or more segments are supported via the XC-DPG503's built-in static routing table.

ARP proxy

The ARP proxy feature allows you to assign an external (Internet) IP address to the XC-DPG503's LAN port. This allows Servers on your LAN to have external (Internet) IP addresses.

Easy Setup

Use your favorite WEB browser for configuration.

Remote Management

The XC-DPG503 can be managed from any PC on your LAN. If the Internet connection exists, the XC-DPG503 can be setup to be configured remotely via the Internet.

Password Protected Configuration

Optional password protection is provided to prevent unauthorized users from modifying the XC-DPG503's configuration data and settings.

HTTP Firmware Upgrade and backup

The web management feature allows you to use HTTP to upgrade new firmware and backup system configuration from local or remote locations.

Email Alert

The XC-DPG503 will send an alert via email to the system administrator in the event a single or both WAN connections go down.

Syslog

Generates real time system information on the web page or sends to a particular computer. This is used for monitoring and diagnosis purposes.

Map Host URL

In addition to the DNS configuration, Map Host URL allows for users to select a URL to map to the IP address of a local host.

QoS Configuration

You will be able to schedule and direct your network traffic to take advantage of your available bandwidth. This function allows for specified packets with higher priority to pass-through such as Internet phone, video conference, and other real-time applications.

UPnP

UPnP dynamically opens and close ports required by certain software automatically.

Physical Details

Front Panel:



Operation of the Front Panel LEDs is as follows:

System:

Power

OFF - No Power.

ON - Normal Operation

Status

OFF - Normal Operation

ON - Firmware not loaded or Hardware Error

Blinking - Data in/out



WAN:

LINK/ACT

ON - Physical connection to the Broadband modem on WAN port 1/2 established.

OFF - No physical connection on WAN port 1/2.

10M/100M

ON - Physical connection using 100BaseT on WAN port 1/2 established.

OFF - 10BaseT connection or no connection on WAN port 1/2.



LAN:

LINK/ACT

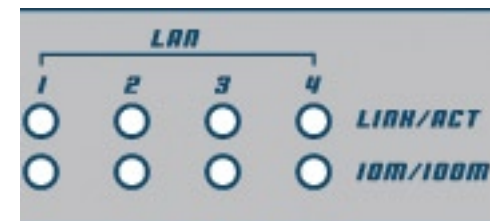
ON - Physical connection or data in/out.

OFF - No physical connection.

10M/100M

ON - The corresponding LAN port is using 100BaseT.

OFF - 10BaseT connection on the corresponding LAN port or no connection.

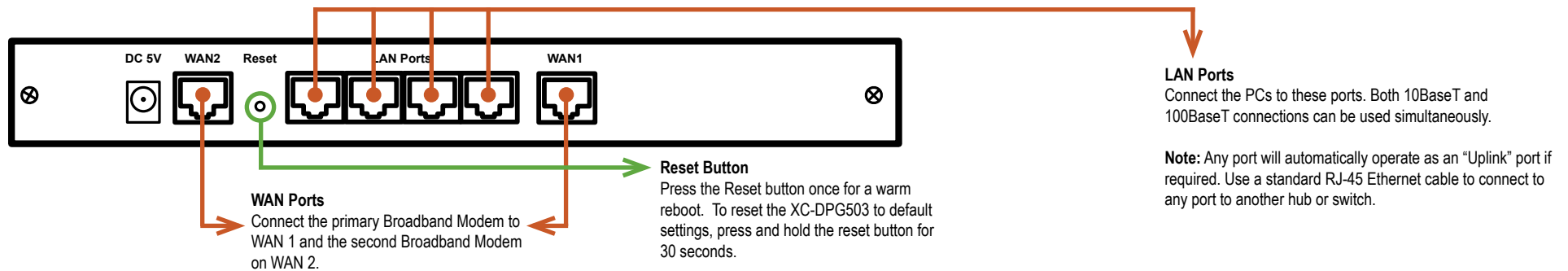


Physical Details

Front Panel Status and Error conditions

LED Action	Condition
WAN1 LINK/ACT & 10M/100M LEDs flash alternatively.	Firmware Download in progress.
WAN1 LINK/ACT & 10M/100M LEDs flash concurrently.	MAC address not assigned.
WAN1 LINK/ACT & 10M/100M LEDs solid On	SDRAM error
WAN2 LINK/ACT & 10M/100M LEDs solid On	Timer/Interrupt error
LAN1 LINK/ACT & 10M/100M LEDs solid On	LAN/WAN error

Rear Panel:



Default Settings

When the XC-DPG503 has finished booting, all configuration settings will be set to the factory defaults, including:

- The IP Address is set to its default value of 192.168.1.1 with a Network Mask of 255.255.255.0
- DHCP Server is enabled
- User Name: admin
- Password cleared (no password)



Chapter 2 - Basic Setup

XC-DPG503 Twin WAN VPN Gateway

Chapter Contents

- Overview
- Procedure
 1. Configuring your LAN
 2. Connecting Broadband Modems
 3. Configuring for Internet Access
 4. Configuring your LAN PCs

Overview

Basic setup of your XC-DPG503 will involve the following steps:

1. Connect the XC-DPG503 to one (1) PC and configure it to your existing LAN.
2. Connecting one or two Broadband Modems to your XC-DPG503.
3. Configuring the XC-DPG503 for Internet Access.
4. Configuring all PCs on your LAN to use the XC-DPG503.

Requirements:

- One or two Broadband modems (T1, xDSL, Cable, and Satellite) with an active account from your ISP(s).
- Two standard 10/100BaseT network (UTP) cables with RJ-45 connectors.
- TCP/IP network protocol must be installed on all PCs.



CAT5 Ethernet Cables



Broadband Modems



TCP/IP Enabled PCs

Configuring the XC-DPG503 for your LAN

Procedure

1. Use a standard LAN cable to connect your PC to any LAN port on the XC-DPG503.
2. Connect the power adapter and power up the XC-DPG503. Only use the power adapter provided with the product; using a different one may cause hardware damage.
3. Start your PC or restart your PC if it is already running. Once restarted, the PC will then obtain an IP address from the XC-DPG503.
4. Start your WEB browser.
5. In the *Address or Location* box enter:
HTTP://192.168.1.1
6. You will be prompted for the User Name and password, as shown in Figure 1.
7. Enter *admin* for the "User Name" and leave the "Password" blank.
 - The *User Name* is always set to **admin**
 - You can and should set a password, using the following Admin Password screen

No Response?

Is your PC using a Fixed IP address?

If so, you must configure your PC to use an IP address within the range 192.168.1.2 to 192.168.1.254, with a Network Mask of 255.255.255.0. See Appendix B – Windows TCP/IP Setup for details.

Be sure to check for the following:

- the XC-DPG503 is properly installed
- the Ethernet cable to the XC-DPG503 is properly attached
- the XC-DPG503 is powered ON

8. After the login, you will then see the Admin Password screen, as shown in Figure 2. Assign a password in both the *Password* and *Verify Password* fields and press the **Submit** button.
9. From the setup menu, select **Basic Setup** and then **LAN & DHCP** from the submenu. You will see a screen like the example in Figure 3.

Figure 1. Password Dialog

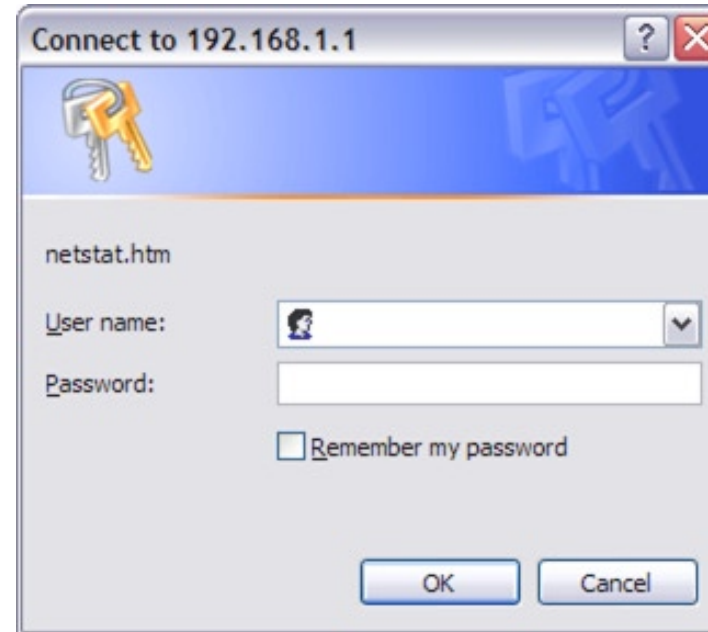


Figure 2. Admin Password



Configuring the XC-DPG503 for your LAN

Ensure these settings are suitable for your LAN:

- The default settings are suitable for many situations.
- See the following table for details of each setting.

Figure 3. LAN & DHCP

Settings - LAN & DHCP

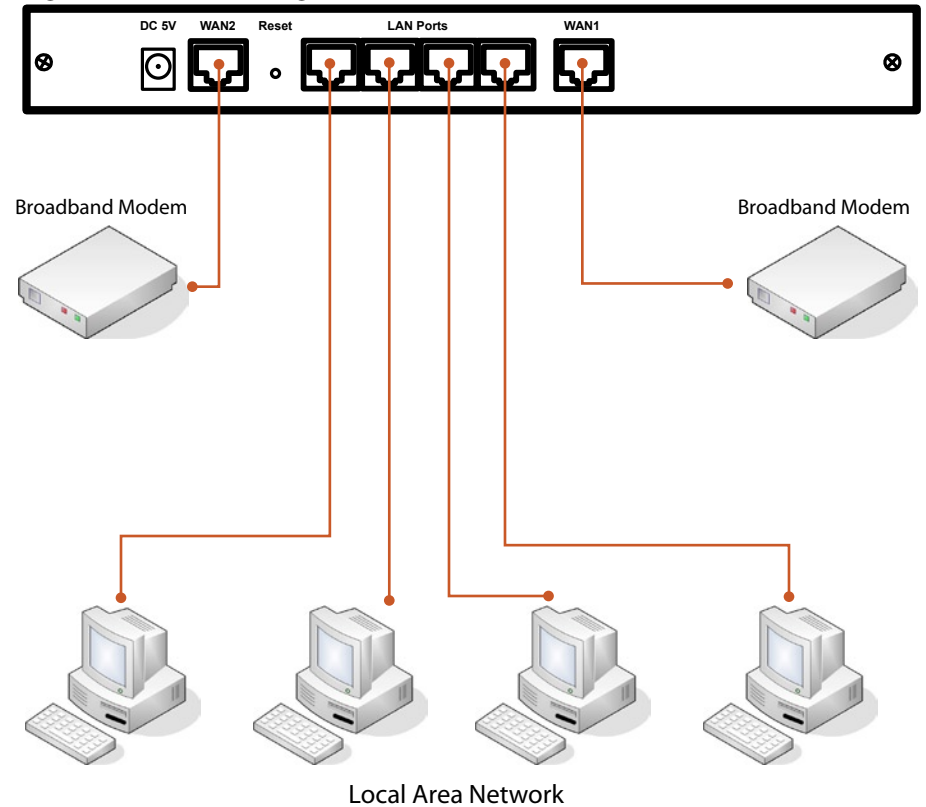
IP Address	This is the IP address for the XC-DPG503 when seen from the local LAN. Use the default value unless the address is already in use or your LAN is using a different IP address range. In the latter case, enter an unused IP Address from within the range used by you LAN
Subnet Mask	The default value 255.255.255.0 is standard for small (class “C”) networks. For other networks, use the Subnet Mask for the LAN segment to which the XC-DPG503 is attached (the same value as the PCs on that LAN segment).
DHCP Server Configuration	<p>DHCP Server Setup - If Enabled, the XC-DPG503 will allocate IP Addresses to PCs (DHCP clients) on your LAN when they start up. The default and recommended value is “Enable”. (Windows systems, by default, act as DHCP clients. This setting is called <i>Obtain an IP address automatically</i>.)</p> <p>DHCP Server Setup - If you are already using a DHCP Server, the DHCP Server setting must be Disabled and the existing DHCP server must be set to provide the IP address of the XC-DPG503 as the <i>Default Gateway</i>.</p> <p>Client Lease Time - A set duration before client’s IP address is released and renewed again after.</p> <p>Client Default DNS – The default DNS which are used by clients. (These settings can be altered)</p>
DHCP IP Address Range	<p>Offered Range fields set the values used by the DHCP server when allocating IP Addresses to DHCP clients. This range also determines the number of DHCP clients supported.</p> <p>Free Entries indicates how many DHCP entries are not currently allocated and are still available.</p>
ARP Proxy	<p>Enable this ONLY if the LAN port has an IP address in the same address range as the WAN port(s). This means that all PCs using this Gateway must have valid fixed external (Internet) IP addresses.</p> <p>If enabled, enter the IP address range used on your LAN.</p>
DHCP Client List	<p>This table shows the IP addresses which have been allocated by the DHCP Server function. For each address which has been allocated, the following information is shown.</p> <p>Name – The “hostname” of the PC. In some cases, this may not be known.</p> <p>MAC Address – The physical address (network adapter address) of the PC.</p> <p>IP Address – The IP address allocated to the PC.</p> <p>Type – Indicates IP address to be dynamic or static.</p> <p>Status – Displays the current status of the DHCP client; either leased or reserved.</p> <p>Time Left – This displays the time left of the leased IP Address.</p>

Connecting two broadband modems

Procedure

1. Ensure the XC-DPG503 and the DSL/Cable modem are powered OFF.
Leave the modem or modems connected to their data line.
2. Connect the Broadband modem(s) to the XC-DPG503.
If using only one (1) Broadband modem, connect it to the "WAN 1" port.
3. Use standard LAN cables to connect PCs to the LAN ports on the XC-DPG503.
 - Both 10BaseT and 100BaseT connections can be used simultaneously.
 - Use a standard CAT-5 Ethernet cable to connect any port on the XC-DPG503 to a standard port on another hub. Any LAN port on the will automatically act as an "Uplink" port when required.
4. Power Up
 - Power on the Cable or DSL modem(s).
 - Connect the supplied power adapter to the XC-DPG503 and power up.
5. Check the LEDs
 - The **Power** LED should be ON.
 - The **WAN – Link** LED should be ON when the corresponding WAN port is connected to a broadband modem.
 - For each PC connected to the LAN ports, the corresponding **LAN** LED (either **10** or **100**) should be ON.

Figure 4. Installation Diagram for XC-DPG503



Configuring for Internet Access

Select Primary Setup from the menu.

1. Configure WAN 1 and/or WAN 2 as required.
2. For any of the following situations, refer to **Chapter 3: Advanced Port Setup** for any further configuration which may be required such as:
 - Using both ports
 - Multiple IP addresses on either port
 - Multiple PPPoE sessions
 - PPTP connection method

Figure 5. Primary Setup Screen

Connection		WAN 1		WAN 2		
Connection Mode	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	<input type="radio"/> Backup	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	<input type="radio"/> Backup
Connection Type	Static IP		Static IP		Static IP	
Address Info. (Static IP only)						
IP Address						
Subnet Mask						
Gateway						
PPPoE / PPTP Dialup (For PPPoE or PPTP)						
PPTP Connection	<input type="checkbox"/> Enable		<input type="checkbox"/> Enable			
PPTP Server IP Address						
User Name						
Password						
Host Name (Optional for PPPoE)						
DNS (Optional for dynamic IP)						
DNS 1						
DNS 2						
DNS 3						
Optional						
Host Name						
Domain Name						
MAC Address	00-09-A3-00-28-EE		00-0E-0B-00-01-38			

Settings - Primary Setup

Connection Mode	Select the appropriate setting: <ul style="list-style-type: none"> • Enable – Select this if you have connected a broadband modem to this port. • Disable – Select this if there is no broadband modem connected to this port. • Backup – Select Enable for the primary port, and Backup for the secondary port. The Backup port will only be used if the primary port fails.
Connection Type	Check the requirements supplied by your ISP, and select the appropriate option. <ul style="list-style-type: none"> • Static IP – Select this if your ISP has provided a Fixed or Static IP address. Then enter the data into the Address Info fields. • Dynamic IP – Select this if your ISP provides an IP address automatically, when you connect. You can ignore the Address Info fields. • PPPoE – Select this if your ISP uses this method (PPPoE software that is usually provided by your ISP is not required to be used when selecting this method). If this method is selected, you must complete the PPPoE dialup fields. Note: If using the PPTP connection method, select Static IP or Dynamic IP to correspond to the IP address method used by your ISP.
Address Info	This is for Static IP users only. Enter the address information provided by your ISP. If your ISP provided multiple IP address, you can use the Multi-DMZ screen to assign the additional IP addresses.
PPPoE / PPTP Dialup	This is for PPPoE and PPTP users only. <ul style="list-style-type: none"> • Enter the Username and Password provided by your ISP. • If using PPTP, enable the PPTP Connection checkbox and enter the IP address of the PPTP server. • Host name (Optional For PPPoE) - This field is used by a Host to uniquely associate an access concentrator to a particular Host request. Note: There are additional PPPoE/PPTP options on the Port Options screen. To use multiple PPPoE sessions on either port, configure the Advanced PPPoE screen.
DNS	If using a Fixed IP address, you MUST enter at least 1 DNS address. If using Dynamic IP or PPPoE, the DNS information is optional.
Optional	<ul style="list-style-type: none"> • Host name – This is required by some ISPs. If your ISP provided a Host Name, enter it here. Otherwise, you can use the default value. • Domain name – This is required by some ISPs. If your ISP provided a Domain Name, enter it here. Otherwise, you can use the default value. • MAC address – Some ISP's record your MAC address (also called "Physical address" or "Network Adapter address").

Setup of the XC-DPG503 is now complete. PCs on your LAN must now be configured. See the following section for details.

Configure PCs on your LAN

Overview

For each PC, the following may need to be configured:

- TCP/IP network settings
- Internet Access configuration

TCP/IP Settings

When using Windows 95/98/ME/2000/XP and the XC-DPG503's TCP/IP default settings, no changes need to be made. Just start or reboot your PC.

- By default, the XC-DPG503 will act as a DHCP Server, automatically providing a suitable IP Address (and related information) to each PC when the PC boots up.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client. In Windows, this is called *Obtain an IP address automatically*. Just start (or restart) your PC, and it will obtain an IP address from the XC-DPG503.
- If using fixed IP addresses on your LAN, or you wish to check your TCP/IP settings, refer to **Appendix B – Windows TCP/IP Setup**.

Internet Access

To configure your PCs to use the XC-DPG503 for Internet access, follow this procedure:

For Windows 9x/2000

1. Select Start Menu > Settings > Control Panel > Internet Options.
2. Select the Connection tab, and click the Setup button.
3. Select *I want to set up my Internet connection manually* or *I want to connect through a local area network (LAN)* and click Next.
4. If *I connect through a local area network (LAN)* is selected, ensure all of the boxes on the following Local area network Internet Configuration screen are unchecked.
5. Check the *No* option when prompted *Do you want to set up an Internet mail account now?*
6. Click Finish to close the Internet Connection Wizard.
Setup is now completed.

For Windows XP

1. Select Start Menu > Control Panel > Network and Internet Connections.
2. Select *Set up or change your Internet Connection*.
3. Select the Connection tab, and click the Setup button.
4. Cancel the pop-up *Location Information* screen.
5. Click Next on the *New Connection Wizard* screen.
6. Select *Connect to the Internet* and click Next.
7. Select *Set up my connection manually* and click Next.
8. Check *Connect using a broadband connection that is always on* and click Next.
9. Click Finish to close the New Connection Wizard.
Setup is now completed.

Accessing AOL

To access AOL (America On Line) through the XC-DPG503, the AOL for Windows software must be configured to use TCP/IP network access, rather than a dial-up connection. The configuration process is as follows:

- Start the AOL for Windows communication software. Ensure that it is Version 2.5, 3.0 or later. This procedure will not work with earlier versions.
- Click the Setup button.
- Select Create Location, and change the location name from "New Locality" to "XC-DPG503".
- Click Edit Location. Select TCP/IP for the Network field. (Leave the Phone Number blank.)
- Click Save, then OK. Configuration is now complete.
- Before clicking "Sign On", always ensure that you are using the "XC-DPG503" location.

Configure PCs on your LAN

For Apple Clients

1. Open the TCP/IP Control Panel.
2. Select Ethernet from the Connect via pop-up menu.
3. Select Using DHCP Server from the Configure pop-up menu. The DHCP Client ID field can be left blank.
4. Close the TCP/IP panel, saving your settings.

Note: If using manually assigned IP addresses instead of DHCP, the required changes are:

- Set the Router Address field to the XC-DPG02's IP Address.
- Ensure your DNS settings are correct.

For Linux Clients

To access the Internet via the XC-DPG503, it is only necessary to set the XC-DPG503 as the "Gateway" and ensure your Name Server settings are correct. **Make sure you are logged in as "root" before attempting any changes.**

Fixed IP Address

By default, most Unix installations use a fixed IP Address. If you wish to continue using a fixed IP Address, make the following changes to your configuration.

Set your Default Gateway to the IP Address of the XC-DPG503.

Ensure your DNS (Name server) settings are correct

To act as a DHCP Client (recommended):

The procedure below may vary according to your version of Linux and X -windows shell.

1. Start your X Windows client.
2. Select Control Panel - Network
3. Select the "Interface" entry for your Network card. Normally, this will be called "eth0".
4. Click the Edit button, set the *protocol* to *DHCP*, and save this data.
5. To apply your changes use the *Deactivate* and *Activate* buttons, if available OR restart your system.



XC-DPG503

Twin WAN VPN Gateway

Chapter Contents

- Overview
- Port Options
- Load Balance
- Advanced PPPoE
- Advanced PPTP

Chapter 3 - Advanced Port

Overview

- **Port Options** contains some options which can be set on either or both WAN ports. For most situations, the default values are satisfactory. Virtual Server
- **Load Balance** screen is only functional if you are using both WAN ports. It allows you to determine the proportion of WAN traffic sent through each port.
- **Advanced PPPoE** setup is required if you wish to use multiple sessions on one or both of the WAN ports. It can also be used to manually connect or disconnect a PPPoE session. Otherwise, this screen can be ignored.
- **Advanced PPTP** setup is required if using the PPTP connection method.

Port Options

Figure 6. Port Options

Connection Validation	WAN 1	WAN 2
Health Check	<input checked="" type="checkbox"/> ICMP <input type="checkbox"/> HTTP	<input checked="" type="checkbox"/> ICMP <input type="checkbox"/> HTTP
Alive Indicator	<input type="text"/>	<input type="text"/>
MTU	1478 Bytes	1478 Bytes
PPPoE/PtP Connection Option	WAN 1	WAN 2
Auto Dialup	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
Auto Disconnect After idle for	0 minutes	0 minutes
Echo Time	30 seconds	30 seconds
Echo Retry	3 times	3 times
Transparent Bridge Option	WAN 1	WAN 2
Bridge Mode	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable
Traffic Management	<input checked="" type="radio"/> Strict Binding <input type="radio"/> Loose Binding <input type="radio"/> Load Balancing	<input type="radio"/> Load Balancing
	<input type="checkbox"/> No IP Translation (For Loose Binding or Load Balancing Mode)	
Arp Tables	32 Entries <input type="button" value="Clear Tables"/>	<input type="button" value="View Tables"/>

Connection Validation	PPPoE / PPTP Connection Options	Transparent Bridge Mode
<p>Health Check Use this field to select the type of connection validation to perform. When set to ICMP, the XC-DPG503 sends out ICMP echo requests. When set to HTTP, the XC-DPG503 requests web pages.</p> <p>Alive Indicator This is the IP address used to check if the WAN connection is operational. When using HTTP, put in a valid IP address of a web server. When this field is blank, the ISP gateway IP address is used. Note: This is not used for PPPoE connections.</p> <p>MTU The Maximum Transmission Unit is used when determining the packet size to be used on the WAN interface. Normally, this does not need to be changed, but if your ISP advises you to use a particular MTU, enter it here.</p>	<p>Auto Dialup When set to Enable a connection will be established whenever outgoing WAN traffic is detected. If not Enabled, you must establish a connection manually.</p> <p>Auto Disconnect This determines when an idle connection will be terminated. Enter the required time period.</p> <p>Echo Time This determines how often an Echo request is sent to the PPPoE server. The Echo request is used to determine if the connection is still valid. Normally, there is no need to change the default value.</p> <p>Echo Retry The number of time the Echo request will be sent if there is no response to the first request. Normally, there is no need to change the default value.</p>	<p>Bridge Mode When set to Enable, this WAN port does not use NAT & Load Balance function when LAN/WAN IP have the real IP addresses on the same network segment.</p> <p>Traffic Management Strict Binding - When a WAN port connection is disconnected, the packets will not go to another WAN port. Loose Binding - When the WAN port connection is connected, the packets will go another WAN port. Load Balancing - This will mix real and private IP's on the LAN side doing the load balancing.</p>

Load Balance

Configuring Load Balancing

The Twin WAN line of products uses a session based Load Balancing algorithm by allowing you to manage sessions using several different options:

- Bytes rx+tx** By monitoring real time speed of both WAN connections, the XC-DPG503 will establish new sessions on the WAN port with the lower speed. Use this if there is a fairly even speed on both lines and would like to benefit the most from the speed available.
- Packets rx+tx** Same as above but in this case, the XC-DPG503 monitors the packet flow and tries to maintain an even number of packets. Use this if transmitting a lot of small packets, such as web browsing and Usenet. This helps you maintain the best latency.
- Sessions Established** The XC-DPG503 tries to maintain an even number of sessions on each WAN port by looking at the current amount of sessions currently established. This is a very general setting only to be used if you have similar types of connections (Cable and Cable, DSL and DSL) to promote good Internet traffic.

Figure 7. Load Balance Console

Load Balance Configuration		
Enable	<input type="checkbox"/>	
Balance Type	Based on Bytes rx+tx	
Loading Share on WAN1	100 %	
<input type="button" value="Update"/>		
NAT Statistics		
	WAN 1	WAN 2
Connection Status	Disconnected	Disconnected
Default Loading Share	100%	0%
Current Loading Share	50 %	50 %
Current Loading	Sessions	1
	Bytes	1
	Packets	1
Current Bandwidth	Download Speed	0Bytes/s
	Upload Speed	0Bytes/s
Interface Statistics		
	WAN 1	WAN 2
Interface Usage	0%	0%
Over All	Bytes received	0KB
	Bytes transmitted	0KB
	Total	0KB

Settings - Load Balance

Load Balance Configuration	<ul style="list-style-type: none"> • Enable – Use this to enable your Load Balance settings. • Balance Type – Select the desired Balance Type: <ul style="list-style-type: none"> - Bytes rx+tx – Traffic is measured by Bytes. - Packets rx+tx – Traffic is measured by Packets. - Sessions established – Traffic is measured by Sessions. • Loading Share on WAN 1 – Enter the percentage (%) of traffic to be sent over WAN 1. The WAN port with the greater bandwidth should be given a higher percentage of traffic over the other WAN port. <p>Click the “<i>Update</i>” button to save your changes.</p>
NAT Statistics	This section displays the current data about WAN 1 and WAN 2. You can use this information to help you “fine-tune” the settings above.
Interface Statistics	This section displays cumulative statistics. Use the “ <i>Restart Counters</i> ” button to restart these counters when required.
Buttons	<ul style="list-style-type: none"> • Update – Save the settings on this screen. • Refresh – Update the data on screen. • Restart Counters – Restart the counters used in the “Interface Statistics” section.

Advanced PPPoE

The screen is required in order to use multiple PPPoE sessions on the same WAN port.

It can also be used to manually connect or disconnect a PPPoE session.

Figure 8. Advanced PPPoE

Connection Status			
WAN	Session	IP Address	Status

Settings - Advanced PPPoE

WAN Port PPPoE Session	Select the desired Port and Session, then click the “ <i>Select</i> ” button. The data for the selected Port/Session will then be displayed in the WAN IP Account section.
WAN IP Account	<ul style="list-style-type: none">• User Name – Enter the PPPoE user name assigned by your ISP.• Password – Enter the PPPoE password assigned by your ISP.• Verify Password – Re-enter the PPPoE password assigned by your ISP.• IP Address – If you have a fixed IP address, enter it here. Otherwise, this field should be left at 0.0.0.0.• Host Name – This field is used by a Host to uniquely associate an access concentrator to a particular Host request.
Action	Use the “ <i>Connect</i> ” and “ <i>Disconnect</i> ” buttons to establish or terminate a connection on this session.
Connection Status	This displays the current connection status for each session.

Advanced PPTP

Figure 9. Advanced PPTP

Select WAN Port & Session			
WAN Port	<input type="text" value="WAN 1"/>	PPPoE Session	<input type="text" value="Session 1"/> <input type="button" value="Select"/>
WAN IP Account			
User Name	<input type="text"/>		
Password	<input type="text"/>		
Verify Password	<input type="text"/>		
IP Address	<input type="text" value="0.0.0.0"/>	(ex. xxx.xxx.xxx.xxx)	
Host Name (Optional)	<input type="text"/>		
Action			
		<input type="button" value="Connect"/>	<input type="button" value="Disconnect"/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>			
Connection Status			
WAN	Session	IP Address	Status

Settings - Advanced PPTP

WAN Port	Select the desired Port and click the "Select" button. The data for the selected Port will then be displayed in the WAN IP Account section.
WAN IP Account	<ul style="list-style-type: none"> • User Name – The PPTP user name (login name) assigned by your ISP. • Password – This field is associated with the <i>User Name</i> above. This is assigned by your ISP and used to login to the PPTP Server. • Verify Password – Re-enter the PPTP password assigned by your ISP. • IP Address – Enter the IP address of the PPTP Server. (This is provided by your ISP) • Static IP Address – If you have a fixed IP address, enter it here. Otherwise, this field should be left at 0.0.0.0.
Action	Use the "Connect" and "Disconnect" buttons to establish or terminate a connection on this session.
Connection Status	This displays the current connection status.



XC-DPG503

Twin WAN VPN Gateway

Chapter Contents

- Host IP Setup
- Virtual Server
- Custom Virtual Server
- Special Applications
- Dynamic DNS
- Multi DMZ
- Advanced Features
- UPnP

Chapter 4 - Advanced Setup

Overview

The following advanced features are provided.

- Host IP Setup
- Virtual Server
- Custom Virtual Server
- Special Applications
- Dynamic DNS
- Multi DMZ
- Advanced Features
- UPnP

This chapter contains details of the configuration and use of each of these features.

Host IP

Host IP

This feature is used in the following situations:

- When you have Multi-Session PPPoE and wish to bind each session to a particular PC on your LAN.
- When you wish to use the Access Filter feature. This requires that each PC be identified by using the Host IP Setup screen.
- When you wish to have different Block URL settings for different PCs. This requires that each PC be identified by using the Host IP Setup screen. (You do not have to use the Host IP feature to apply the same Block URL settings to all PCs.)
- When you wish to reserve a particular (LAN) IP address for a particular PC on your LAN. This allows the PC to use DHCP (Windows calls this “Obtain an IP address automatically”) while gaining the benefits of a fixed IP address. The PC’s IP address will never change, so it can be provided to other people and applications.

Settings - Host IP Setup

Host Network Identity	<p>This section identifies each Host (PC)</p> <ul style="list-style-type: none">• Host List – Ignore this list when adding a new Host. To edit an existing entry, select it from the list and click the “<i>Select</i>” button. The data fields will then be updated with data for the selected entry.• Host name – Enter a suitable name. Generally, you should use the “<i>Host name</i>” (computer name) defined on the Host itself.• MAC Address – Also called Physical Address or Network Adapter Address. Enter the MAC address of this host.• Select Group – Select the group you wish to put this host into.• Reserve in DHCP – Select <i>Enable</i> to reserve a particular (LAN) IP address for a particular PC on your LAN. This allows the PC to use DHCP (Windows calls this <i>Obtain an IP address automatically</i>) while having an IP address which never changes.• Reserved IP – If the setting above is <i>Enabled</i>, enter the IP address you wish to reserve. Otherwise, ignore this field.
Host Network Binding	<ul style="list-style-type: none">• Bind WAN port/Session – Select <i>Enable</i> if you wish to associate this PC with a particular PPPoE Session. All traffic for that PC will then use the selected PPPoE port and session.• Binding Method – Strict Binding - no failover Loose Binding - failover only Load Balancing - load balancing & failover• Select WAN Port/Select PPPoE session – If the setting above is <i>Enable</i>, select the desired Port and Session. Otherwise, ignore these settings. <p>Note: Multiple PPPoE sessions are defined on the Advanced PPPoE screen.</p>
Buttons	<ul style="list-style-type: none">• Add – Use this to add a new entry to the database, using the data shown on screen.• Delete – Click this to delete the selected entry.• Update – Use this to update the selected entry, after making the desired changes.• Reset – Reverse any changes you have made since loading the data from the XC-DPG503.
Host & Group List	<p>This table shows the current bindings.</p>

Virtual Servers

Virtual Servers

This feature allows you to make Servers on your LAN accessible to Internet users. Normally, Internet users would not be able to access a server on your LAN because:

- Your Server's IP address is only valid on your LAN, not on the Internet.
- Attempts to connect to devices on your LAN are blocked by the firewall in the XC-DPG503.

The "Virtual Server" feature solves these problems and allows Internet users to connect to your servers, as illustrated in Figure 10.

Connecting to Virtual Servers

Once configured, anyone on the Internet can connect to your Virtual Servers. They must use the XC-DPG503's Internet IP Address (the IP Address provided by your ISP).

Example:

`http://205.20.45.34`

`ftp://205.20.45.34`

- To Internet users, all virtual Servers on your LAN have the same IP Address. This IP Address is allocated by your ISP.
- This address should be static, rather than dynamic, to make it easier for Internet users to connect to your Servers. However, you can use the Dynamic DNS feature (explained later in this chapter) to allow users to connect to your Virtual Servers using a URL, instead of an IP Address.

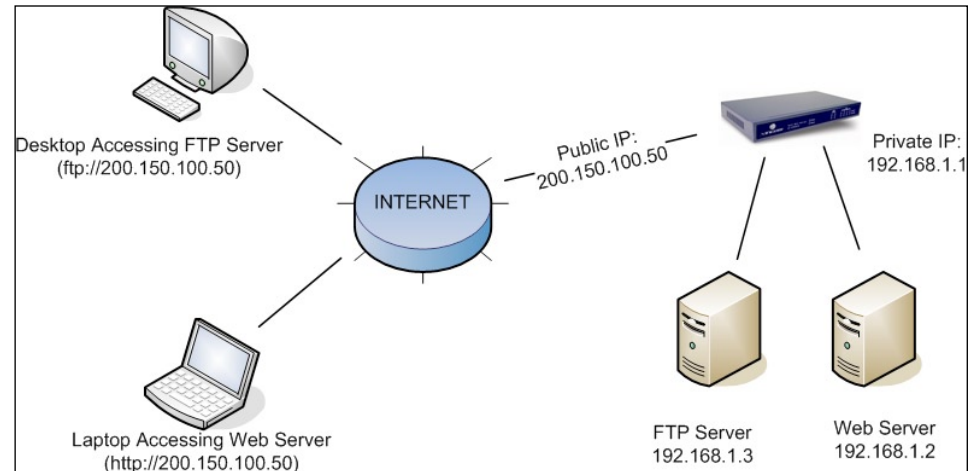
e.g. `HTTP://my_domain_name.dyndns.org`

`FTP://my_domain_name.dyndns.org`

Settings - Virtual Server

Enable	Use this to Enable or Disable each Virtual server as required.
Server Type	Select the desired Server type. If the type of Server you wish to use is not listed, use the Custom Virtual Server screen to define your own type.
LAN IP Address	Enter the IP address of the PC on your LAN which is running the required Server software. Each PC should have a fixed IP address, or have a reserved IP address. (See the Host IP section earlier in this chapter for details on reserving an IP address.)

Figure 10. Virtual Servers



Note: In this illustration, both Internet users are connecting to the same IP Address but using different protocols.

Custom Virtual Servers

Custom Virtual Servers

This screen allows you to define your own Server types. This is for situations when the desired Server type is not listed on the Virtual Servers screen.

Settings - Custom Virtual Servers

Select Custom Server Name	Server List If creating a new entry, ignore this list. To edit an existing entry, select it, and then click the “ <i>Select</i> ” button. The screen will update with data for the selected entry.
Custom Server Configuration	This data defines the Custom Virtual Server: <ul style="list-style-type: none">• Server Name – Enter a suitable name for this server.• State – Use this to Enable or Disable the server.• Server IP – Enter the IP address of the PC on you LAN which is running the required Server software. Each PC should have a fixed IP address or have a reserved IP address. (See the Host IP section earlier in this Chapter for details on reserving an IP address). Each PC must be running the appropriate Server software.• Protocol Type – Select the network protocol used by this sever type.• LAN Port Range – Enter the range of port number used for outgoing traffic from this Server. If only a single port is required, enter it in both fields.• WAN Port Range – Enter the range of port number used for incoming traffic to this Server. If only a single port is required, enter it in both fields• Interface Binding – This selection allows the servers to be bound to WAN1, WAN2, or both ports together.
Buttons	<ul style="list-style-type: none">• Add – Create a new Special Application entry.• Delete – Delete the selected entry.• Update – Save any changes you have made to the current entry.• Cancel – Cancel any changes you have made since the last save operation.
Custom Virtual Server List	This table shows details of all defined Custom Virtual Servers.

Special Applications

Special Application

If you use Internet applications which have non-standard connections or port numbers, you may find that they do not function correctly because they are blocked by the XC-DPG503 firewall. In this case, you can define the application as a “Special Application” in order to make it work.

Note that the terms “Incoming” and “Outgoing” on this screen refer to traffic from the client (PC) viewpoint.

Settings - Special Applications

Select Special Application Name	
Select Name Item	This lists any special applications which are currently defined. <ul style="list-style-type: none">• Ignore this list if adding a new Special Application. Enter your data in the Special Application Configuration section, and click the “Add” button.• To edit an existing entry select it from this list and click the “Select” button. The data for the selected application will then be displayed in the Special Application Configuration section. Make any required changes and then click the “Update” button.
Special Application Configuration	
Enable	Use this to Enable or Disable the Special Application.
Name	Enter a descriptive name to identify this Special Application.
Outgoing Protocol	Select the protocol used by this application when sending data to the remote server or PC.
Outgoing Port Range	For data being sent, enter the beginning and end of the range of port numbers used by the application server. If the application uses a single port number, enter the range in both fields.
Incoming Protocol	Select the protocol used by this application, when receiving data from the remote server or PC.
Incoming Port Range	For data being recieved, enter the beginning and end of the range of port numbers used by the application server. If the application uses a single port number, enter it in both fields.
Buttons	<ul style="list-style-type: none">• Add – Create a new Special Application entry.• Delete – Delete the selected entry.• Update – Save any changes you have made to the current entry.• Cancel – Cancel any changes you have made since the last save operation.
Special Application List	This shows details of all Special Applications which are currently defined.

Using a Special Application on your PC

- Once the Special Applications screen is configured correctly, you can use the application on your PC normally. Remember that only one (1) PC can use each Special application at any time.
- Also, when 1 PC is finished using a particular Special Application, there may need to be a “Time-out” period before another PC can use the same Special Application.
- If an application still cannot function correctly, try using the “DMZ” feature, if possible.

Dynamic DNS

Dynamic DNS

Dynamic DNS is very useful when combined with the Virtual Server feature. It allows Internet users to connect to your Virtual Servers using a URL, rather than an IP Address. This also solves the problem of having a dynamic IP address. With a dynamic IP address, your IP address may change whenever you connect to your ISP.

You must register for the Dynamic DNS service. The XC-DPG503 supports 2 types of service providers:

- Standard client, available at <http://www.dyndns.org>.
Other sites may offer the same service, but can not be guaranteed to work.
- TZO at <http://www.tzo.com>
- 3322 is available in China at <http://www.3322.org>

To use the Dynamic DNS Feature:

1. Register for the service from your preferred service provider.
2. Follow the service provider's procedure to have a Domain Name (Host name) allocated to you.
3. Configure the appropriate settings in the Dynamic DNS screen
4. The XC-DPG503 will then automatically update your IP Address recorded by the Dynamic DNS service provider.
5. From the Internet, users will now be able to connect to your Virtual Servers (or DMZ PC) using your Domain name.

Settings - Dynamic DNS

Dynamic DNS Service	Use this to Enable/Disable the Dynamic DNS feature and select the required service provider. <ul style="list-style-type: none">• Disable – Dynamic DNS is not used.• TZO – Select this to use the TZO service (www.tzo.com). You must configure the TZO section of this screen.• Standard Client – Select this to use the standard service (from www.dyndns.org or other provider). You must configure the Standard Client section of this screen.• 3322 (in China) – This is available in China. It is similar to "Standard client"
WAN Port Binding	<ul style="list-style-type: none">• Select the WAN port on which the Dynamic DNS is used.• The "Force Update" button will update your record on the Dynamic DNS Server immediately.
TZO Custom Dynamic DNS Service	If you have registered for this service, complete these fields: <ul style="list-style-type: none">• Key – Enter your Key as recorded on the TZO Web site.• E-mail – Enter your E-mail address as recorded on the TZO Web site.• Domain – Enter the domain name allocated to you by TZO.
Standard Client or 3322	If you have registered for this service, complete these fields. <ul style="list-style-type: none">• User Name – Enter the user name given by the service provider.• Password – Enter the password given by the service provider.• Verity Password – Re-enter the password above.• Server – Enter the name or IP address of the service provider's server.• Host Name - Enter the domain name allocated to you by the service provider.
Additional Standard Client or 3322 Settings	These options are available if using the standard client. <ul style="list-style-type: none">• Enable Wildcard – If selected, traffic sent to sub-domains (of your Domain name) will also be forwarded to you.• Enable backup MX – If enabled, you must enter the Mail Exchanger address below.• Mail Exchanger – If the setting above is enabled, enter the address of the backup Mail Exchanger.

Multi DMZ & UPnP

Dynamic DNS

This feature allows each WAN port IP address to be associated with one (1) computer on your LAN. All outgoing traffic from that PC will be associated with that WAN port IP address. Any traffic sent to that IP address will be forwarded to the specified PC. This allows unrestricted 2-way communication between the “DMZ PC” and other Internet users or Servers.

Note:

The “DMZ PC” is effectively outside the Firewall making it more vulnerable to attacks. Enable the DMZ feature when required.

Settings - Multi DMZ

Enable	Use this to enable or disable the DMZ setting when required.
Name	Enter a name to assist you to remember this setting. This name has no effect on the operation.
For Static IP	
Public IP Address	Enter the WAN port (Internet) IP address you wish to associate to a PC. This IP address must have been allocated to you by your ISP.
Private IP Address (LAN)	Enter the IP address of the PC you wish to associate with this WAN port IP address. This IP address should be fixed, or reserved. (See the Host IP section for details on reserving an IP address.)
For Dynamic IP	
WAN	Select the desired WAN port.
Session	<ul style="list-style-type: none">• Select “DHCP” if the IP address on this WAN port is dynamically assigned. You can only select assign one (1) Private (LAN) IP address to each port.• If using multi-session PPPoE, select the desired PPPoE session. These sessions are defined on the Advanced PPPoE screen. You can assign one (1) Private (LAN) IP address to each PPPoE session.
Private IP Address (LAN)	Enter the IP address of the PC you wish to associate with this WAN port IP address. This IP address should be fixed or reserved. (See the Host IP section for details on reserving an IP address)
Access Group	You can decide the users to have the authority of using DMZ by defining the groups.
Direction	For DMZ, you can allow inbound, outbound only, or both inbound and outbound.

UPnP

The UPnP (Universal Plug & Play) function can easily setup and configure an entire network, enable discovery, and control network devices and services.

When UPnP is enabled, an DPG503 icon will show up on network neighborhood (Microsoft Windows OS). Every time you add a new network device with port mapping, the new network device will appear on the mapping list.

Advanced Features

Advanced Features

- **NAT** – NAT (Network Address Translation) is the technology which allows a number of LAN PCs to share one (1) Internet IP address.
- **Remote Access Configuration** – This feature allows you to manage the XC-DPG503 via the Internet. You can restrict access to a specified IP address or address range.
- **External Filters Configuration** – These settings determine whether or not the XC-DPG503 should respond to ICMP (ping) requests received from the WAN port.
- **Interface Binding** – Use these to ensure that certain traffic is sent by a particular WAN port, and thereby a particular ISP account. These settings are only useful if using both WAN ports.
- **Protocol & Port Binding** – This allows you binding WAN 1 or WAN 2 ports by selecting TCP/UDP protocol

Settings - Advanced Features

NAT Configuration	<ul style="list-style-type: none"> • NAT Routing – NAT (Network Address Translation) is the technology which allows one (1) WAN (Internet) IP address to be used by many LAN users. <ul style="list-style-type: none"> - If you disable NAT, Internet access is only possible if all PCs are configured with valid Internet IP addresses. (The XC-DPG503 needs 2 addresses: 1 for the LAN port and 1 for the WAN port.) - NAT is disabled only when you wish to use the XC-DPG503 as a Static Router. • TCP Timeout – Enter the desired value to use on both WAN ports. The default is 300. • UDP Timeout – Enter the desired value to use on both WAN ports. The default is 120. • TCP Window Limit – Enter the desired value to use on both WAN ports. The default is 0 (no limit). • TCP MSS Limit – Enter the required MSS (Maximum Segment Size) to use on both WAN ports. The default is 0 (no limit). • Disable Port Translation – Enter the desired port range of all packets which are not translated via WAN port.
Remote Access Configuration	<ul style="list-style-type: none"> • Remote Upgrade – If enabled, you can <input type="checkbox"/> • Remote Web-based setup – If enabled, access to the Web-based interface is available via the Internet. If not enabled, access is only available to PCs on the LAN. • Port – The port number used when connecting remotely. See below for details. • Allowed IP range – Remote access is only available to the IP addresses entered here. <ul style="list-style-type: none"> - Leaving these fields blank will allow access by all PCs. - These addresses must be Internet IP addresses and not addresses on the local LAN. - To specify a single address, enter it in both fields.
External Filters Configuration	<p>These settings determine whether or not the XC-DPG503 should respond to ICMP (ping) requests received from the WAN port.</p> <ul style="list-style-type: none"> • Block Selected packet types – This acts as “master” switch. If checked, the selected packet types are blocked. Otherwise, they are accepted. • Echo Request, Timestamp Request – Select the packet types you wish to block, using the checkboxes.
Dynamic Routing	<ul style="list-style-type: none"> • RIP v2 – This acts as “master” switch. If enabled, the selected WAN or LAN will run RIPv1/v2. • LAN, WAN1, WAN2 – When enabled, any WAN or LAN can execute RIP function.
DNS Loopback	<p>Some servers on a LAN and their domain names have already registered on public DNS. To avoid DNS loopback problem, enter the following fields.</p> <ul style="list-style-type: none"> • Domain Name – Enter the domain name specified by you for local host/server. • Private IP – Enter the private IP address of your local host/server.
Interface Binding	<p>SMTP (Simple Mail Transport Protocol) Binding (This applies only when using E-mail accounts from different ISPs on each port) Some ISPs configure their E-mail Servers so they will not accept E-mail from IP addresses not allocated by themselves. If you are using accounts from different ISPs, sending E-mail over the wrong port may result in non-acceptance of the mail. In this case, you can use these settings to correct the problem.</p> <ul style="list-style-type: none"> • Enable - When enabled, the port you specify below will be used for all outgoing SMTP traffic. If not enabled, either port will be used. • WAN 1 / WAN 2 – Select the desired port.
Protocol & Port Binding	<p>Use these settings if you wish to ensure user-defined traffic to be sent by a specific WAN port. This allows that user-defined traffic to be handled by a designated ISP account.</p> <ul style="list-style-type: none"> • Enable - Enable or disable each item as required. • Source IP - IP address of source which packets are sent from. • Destination IP – IP address of destination which packets are sent to. • Subnet Mask – With subnet mask other than 255.255.255.255, you can make a IP sub-network as your destination. • Protocol - Select the protocol used by the traffic you wish to configure. • Port Range - Enter the beginning and end of the port range used by the traffic you wish to configure. If only a single port is used, enter the port number in both fields. • WAN - Select the port you wish this traffic to use.

Advanced Features (continued)

Using Remote Web-based Setup

To connect to the XC-DPG503 from a remote PC via the Internet:

1. Ensure that both your PC and the XC-DPG503 are connected to the Internet.
2. Start your Web Browser.
3. In the Address bar enter:

HTTP:// (Internet IP Address of the XC-DPG503)

The Port number is also required. (After the IP Address, enter “:” followed by the port number.)

e.g.: HTTP://123.123.123.123:8080

- This example assumes the WAN IP Address is 123.123.123.123, and the port number is 8080.
- If using the Dynamic DNS feature, you can connect using the domain name allocated to you.
e.g.: HTTP://my_domain_name.dyndns.org:8080



XC-DPG503

Twin WAN VPN Gateway

Chapter Contents

- Block URL
- Access Filter
- Session Limit
- Firewall Exception

Chapter 5 - Security Management

Overview

- **Block URL** - This feature blocks specific web sites by IP address, URL, or keywords.
- **Access Filter** - Block all Internet access, well-known ports, or block user define ports by groups.
- **Session Limit** - Eliminate users' Internet access and send email alert to the administrator if the device detects new sessions that exceeds the maximum sampling time.
- **Firewall Exception**

Block URL

Block URL

This feature allows you to block access to undesirable Web sites. You can block by URL, IP address, or Keyword. You can also have different blocking settings for different groups of PCs.

- Every URL is searched to see if it matches or contains any of the URL or keywords entered here. After a DNS lookup determines the IP address of the requested site, the site's IP address is checked against IP address entries on this screen.
- Note that a single IP address may host many Web sites. Entering the IP address on this screen will block all Web sites hosted on that IP address.

Settings - Block URL

Access Group	This allows you have different blocking rules for different Groups of PCs. <ul style="list-style-type: none">• All PCs (users) are in the Default Group unless moved to another group on the Host IP screen.• If you want the same restrictions to apply to everyone, select Default for the Group. In this case, there is no need to enter any Hosts on the Host IP screen.• If you wish to apply different restrictions on different Groups, select the desired Group, and click the "Select" button. The screen will update with data for the selected Group.
Block Internet Access	<ul style="list-style-type: none">• Enable/Disable – Use this to Enable or Disable each setting as needed.• Block URL/IP/Keyword – Enter the URL IP address or keyword you wish to block.

Access Filter

The network Administrator can use the Access Filter to gain fine control over the Internet access and applications available to LAN users.

- Five (5) user groups are available and each group can have different access rights.
- All PCs (users) are in the Default group unless assigned to another group on the Host IP screen.

Settings - Access Filter

Setup Access Group	This allows you have different access rights for different Groups of PCs. <ul style="list-style-type: none">• If you want the same restrictions to apply to everyone, select Default for the Group. In this case, there is no need to enter any Hosts on the Host IP screen.• If you wish to apply different restrictions on different Groups, select the desired Group, and click the "Select" button. The screen will update with data for the selected Group.
Filter Setting	Select the desired option for this Group: <ul style="list-style-type: none">• No filtering – Nothing is blocked; Internet access is not restricted.• Block All Access – Everything is blocked; Internet access is not available.• Block selected items – Items selected on this screen are blocked. You can block well known services by using the check boxes, or define your own filters.
Block well known ports	Select the services you wish to block. The current group will not be able to use any services which are checked.
User-defined Ports to Block	This section is optional. It allows you to define your own filters if required. For each filter, the following information is required. <ul style="list-style-type: none">• Name – Enter a name for this filter.• TPC/UDP Packets – Select either TCP or UDP, depending on which protocol is used by the service you wish to block.• Port No. Range – Enter the range of port numbers used by the service you wish to block. If only a single port is required, enter it in both fields.

Session Limit & Firewall Exception

Session Limit

This new feature allows to drop the new sessions from both WAN and LAN side. If the new sessions number are exceed the maximum sessions in a sampling time.

Settings - Session Limit

Sample Time	The period to count the new session. Only those new sessions occurred in the most recently sampling time were be count for limit checking. (Default is 400 mil-sec)
Maximum of Total New session	If the number of new sessions for system exceed the maximum in the Sampling Time. Any new sessions in the system will be dropped. (Default: 65535 session/sec)
Maximum of New Sessions for Host	If the number of new sessions for the host exceeds the maximum in the sampling time. Any new session of the host will be dropped. (Default: session/sec)
Maximum of Dropped New Sessions for Host	If the number of dropped new sessions for the host exceeds the Maximum in the sampling time, any new session of the host will be dropped for the pause time.
Pause Time	Within the pause time, no new session of the suspended host could be served by system.(Default is 5 minutes)

Firewall Exception

System Firewall Exception Rules: The rules with which any received packets is complied, the packets will not processed by Firewall or NAT module, but to be processed directly by system protocol stack.

Settings - Firewall Exception

Enable	The check box can allow you enable or disable firewall exception.
Interface	You can select LAN, WAN1, WAN2 or ALL interfaces to be process by the system protocol stack.
Protocol	There are six protocols (UDP/TCP/ICMP/GRE/ESP/AH) to choose from. This allows packets to be directly processed by the system protocol stack.
Foreign Port Range	Select foreign port number range directly process by system protocol stack. Click the check box to enable.
Device Port Range	Select device port number range directly process by system protocol stack. Click the check box to enable.



Chapter 6 - QoS Configuration

Overview

The XC-DPG503 provides QoS, which supports the high quality of network service. Classifying outgoing packets based on some policies defined by users provides real-time applications to get better response or performance.

Settings - QoS Setup

QoS Feature	<ul style="list-style-type: none"> • Enable QoS – This will allow users enable QoS function. • Queuing Method – The methods that how you manage your queue- Priority queuing. It is one of the first queuing variations to be widely implemented
IP TOS (Type of Service) Feature	<ul style="list-style-type: none"> • Process TOS Field –An 8-bit field in the IP packet header designed to contain values indicating how each packet should be handled in the network. If you choose “enable” then it will enable this function to process the IP Type of Service field. • Overwrite policy priority – Choose “yes” to set the priority of the TOS field in IP packet overwrite the priority defined in policy configuration

Policy Configuration

When you use QoS, you must define some policies to make some packets to have higher priority to pass through.

Settings - Policy Configuration

Network Admission Policy
<p>This section identifies each policy:</p> <p>Policy Name List – Ignore this list when adding a new Policy. To edit an existing entry, select it from the list and click the “Select” button. The data fields will then be updated with data for the selected entry.</p> <p>Policy Name – Enter a suitable name. Generally, you should use the “Policy Name” for the network traffic.</p> <p>Source Address – Define the source address of packets here. It has two types like IP address or MAC address. If you select IP address, you can define IP address range. Otherwise you may define up to four MAC addresses.</p> <p>Destination Address – Define the destination address of packets here. The explanation is as the same as above.</p> <p>Protocol Type – The field defines traffic packet type, i.e. IP,TCP and UDP.</p> <p>Source Port – Define the source port of packets here.</p> <p>Destination Port – Define the destination port of packets here.</p> <p>Priority Queue – This defines a packet. If it meets all conditions defined above, it will be serviced with some priority level.</p>

XC-DPG503 Twin WAN VPN Gateway

Chapter Contents

- Overview
- QoS Setup
- Policy Configuration



XC-DPG503 Twin WAN VPN Gateway

Chapter Contents

- Overview
- IPSec Global Setting
- Policy Setup

Chapter 7 - VPN Configuration

Overview

Virtual Private Network (VPN) uses encryption to connect computers over a public network such as the Internet. Encrypted connections between computers are commonly referred to as a *tunnel*. These secure tunnels permit sending private data from one computer to another without the risk of unauthorized access from outside intruders. Combined with low cost and straight forward configuration, the XC-DPG503 makes VPN a perfect alternative to private communication lines.

XiNCOM XC-DPG503 is a VPN capable Dual WAN Gateway with industry standard IPsec encryption. It provides extremely secure LAN-to-LAN connectivity over the Internet. The 503 supports VPN by encryption, encapsulation, and authentication using the following methods: DES/3DES/AES, MD5, SHA-1 and SHA-2; up to 50 IPsec tunnels are permitted.

The VPN configuration menu allows you to configure the behavior of the XiNCOM XC-DPG503. Before creating a configuration, please review your requirement for VPN:

- Is this going to be a Client – to – Gateway VPN or a Gateway – to – Gateway VPN?
- What type of authentication would you be using? (DES, 3DES or AES)
- How many computers do you want to have access to the VPN?

Note:

The XC-DPG503 uses the IPsec VPN protocol. However, due to variations in how manufactures interpret this protocol standard, not all VPN products are interoperable with each other. Although the Twin WAN VPN Gateway can interoperate with many other VPN products, XiNCOM cannot to provide specific support for all other products.

IPSec Global Settings

IPSec Global Setting

IP Global Setting

Enable

Enabling either WAN 1, WAN 2, or both will start the VPN global setting.

ISAKmp Port

Internet Security Association and Key Protocol Management (ISAKmp) is designed to negotiate, establish, modify, and delete security associations and their attributes. In particular, it was assigned UDP port 500 by the IANA.

Phase 1 DH Group

Use DH Group 1(768-bits),DH Group 2(1024-bits), Group 5 (1536-bits) to generate IPSec SA keys.

Phase 1 Encryption Method

There are three data encryption methods available, DES, 3DES, and AES.

Phase 1 Authentication Method

There are two authentication available. MD5 and SHA1 (Secure Hash Algorithm)

Phase 1 SA Life Time

By default the Security Association lifetime is set at 28800 Sec.

Maxtime to complete phase 1

The aim of phase 1 is to authenticate and establish a secure tunnel, which will protect further IKE negotiation. The maximum time default is 30 sec.

Maxtime to complete phase 2

Maximum time to establish the IPSec SAs. By default the maximum time is 30 sec.

Log Level

Select a VPN log level that you like to display on VPN log.

IPSec Global Setting



IPSec Global Setting	WAN1	WAN2
Enable	<input type="checkbox"/>	<input type="checkbox"/>
ISAKmp Port	500	500
Phase 1 DH Group	DH Group 2	DH Group 2
Phase 1 Encryption Method	DES	DES
Phase 1 Authentication Method	MD5	MD5
Phase 1 SA Lifetime	28800 Seconds	28800 Seconds
Retry Counter	5	5
Retry Interval	10 Seconds	10 Seconds
Maxtime to complete Phase 1	30 Seconds	30 Seconds
Maxtime to complete Phase 2	30 Seconds	30 Seconds
Count Per Second	1	1

Log Level
Log Level

Trace

Submit Reset

Planning the VPN

Consider these questions and setups when planning your VPN:

- If the remote end is a LAN network, the two-endpoint network must have different LAN IP address ranges. If the remote endpoint is a single PC running a VPN client, its destination address must be a single IP address, with subnet mask of 255.255.255.255
- Will you be using the Internet Key Exchange (IKE) setup or Manual Keying? For either method, you must specify each phase of the connection.
- At least one side must have a fixed IP address. The other side with a dynamic IP address must always be the initiator of the connection.
- What encryption level will you use? (DES/3DES - hardware encryption; AES - software encryption)

Policy Setup

Policy Setup



IPSec Traffic Binding							
VPN Tunnel List	<input type="text"/>						
Tunnel Name	<input type="text"/>						
Tunnel	<input type="checkbox"/> Enable						
WAN Port	Any						
PPPoE Session	Session 1						
Traffic Selector							
Service	Protocol Type: Any, Local Type: Subnet						
Local Security Network	IP Address: 0.0.0.0, Mask Address: 0.0.0.0, Port Range: 0 ~ 0						
Remote Security Network	Remote Type: Subnet, IP Address: 0.0.0.0, Mask Address: 0.0.0.0, Port Range: 0 ~ 0						
Remote Security Gateway	Gateway Type: IP Address, IP Address: 0.0.0.0						
Security Level							
Encryption Method	NULL						
Authentication Method	NULL						
Remote Security Gateway	Gateway Type: IP Address, IP Address: 0.0.0.0						
Security Level							
Encryption Method	NULL						
Authentication Method	NULL						
Key Management							
Key Type	Manual Key						
Encryption Key	<input type="text"/> (Char.)						
Authentication Key	<input type="text"/> (Char.)						
Inbound SPI	0x0 (Dec / Hex:0x)						
Outbound SPI	0x0 (Dec / Hex:0x)						
Options							
NetBIOS Broadcast	<input checked="" type="checkbox"/> Enable						
Keep Alive	<input type="checkbox"/> Enable						
Anti Replay	<input type="checkbox"/> Enable						
Passive Mode	<input type="checkbox"/> Enable						
Check ESP Pad	<input type="checkbox"/> Enable						
Allow Full ECN	<input type="checkbox"/> Enable						
Copy DF Flag	<input type="checkbox"/> Enable						
Set DF Flag	<input type="checkbox"/> Enable						
Action							
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Update"/> <input type="button" value="Reset"/>							
Security Association List							
State	Name	Security Gateway	Remote Site	Security Policy	Key Type	WAN	Status
<input type="button" value="Previous Page"/> <input type="button" value="Next Page"/> <input type="button" value="Refresh"/>							

VPN Policy Setup

IPSec Traffic Binding

VPN Tunnel List

It shows the tunnels that you have entered. The router can setup up to 50 tunnels

Tunnel Name

This distinguishes different "tunnels" by name.

Tunnel

The tunnel can only be connected when the **Enable** check box is selected.

WAN port

You can choose WAN1, WAN2 or Any to make the VPN connection.

PPPoE Session

Some ISPs offer multiple sessions when using PPPoE to make the VPN connection. You can select these PPPoE sessions to construct VPN tunnels.

Traffic Selector

Service

Protocol Type: You can choose either TCP/UDP/ICMP/GRE protocol as your connection protocol. By default the protocol type is "Any".

Local Security Network

These entries identify the private network on the VPN gateway and the hosts of which can use the LAN-to-LAN connection. You can choose a single IP address, the subnet, or a selected IP range to make VPN LAN-to-LAN connection.

Remote Security Network

These entries identify the private network on the remote peer VPN router whose hosts can use the LAN-to-LAN connection. You can choose a single IP address, the subnet, or a selected IP range to make VPN connection

Remote Security Gateway

You can either select remote side domain name or remote side IP address (WAN IP address) as your remote side security gateway.

Security Level

Encryption Method

It specifies the encryption mechanism to use. Data encryption makes the data unreadable if intercepted. There are three encryption method available: DES, 3DES and AES. The default is null.

Authentication

This specifies the packet authentication mechanism to use. Packet authentication confirms the data's source. There are three authentications available: MD5, SHA1 and SHA2.

Policy Setup

VPN Policy Setup (continued)

Key Management	
<p>Key - Key Type: There are two key types (manual key and auto key) available for the key exchange management.</p> <ul style="list-style-type: none"> ○ Manual Key: If manual key is selected, no key negotiation is needed. <ul style="list-style-type: none"> □ Encryption Key - This field specifies a key to encrypt and decrypt IP traffic. □ Authentication Key - This field specifies a key use to authentication IP traffic. □ Inbound/outbound SPI (Security Parameter Index) is carried on the ESP header. Each tunnel must have a unique inbound and outbound SPI and no two tunnels share the same SPI. Notice that Inbound SPI must match the other router's outbound SPI. ○ AutoKey (IKE) - There are two types of operation modes can be used: <ul style="list-style-type: none"> □ Main mode accomplishes a phase one IKE exchange by establishing a secure channel. □ Aggressive Mode is another way of accomplishing a phase one exchange. It is faster and simpler than main mode, but does not provide identity protection for the negotiating nodes. 	
Perfect Forward Secrecy (PFS)	If PFS is enable, IKE phase 2 negotiation will generate a new key material for IP traffic encryption & authentication.
Preshared Key	This field is to authenticate the remote IKE peer.
Key Lifetime	This specifies the lifetime of the IKE generated Key. If the time expires or data is passed over this volume, a new key will be renegotiated. By default, 0 is set for no limit.
Options	
NetBIOS Broadcast	This is used to forward NetBIOS broadcast across the Internet.
Keep Alive	This is to help maintain the IPSec connection tunnel. It can be re-established immediately if a connection is dropped.
Anti Replay	The Anti Replay mechanism works by keeping track of the sequence numbers in packets as they arrive.
Passive Mode	When enabled, your PC establishes the data connection.
Check ESP Pad	When checked, this will enable ESP (Encapsulating Security Payload) padding.
Allow Full ECN	Enable will allow full Explicit Congestion Notification (ECN). ECN is a standard proposed by the IETF that will minimize congestion on network and the gateway dropping packets.
Copy DF Flag	When an IP packet is encapsulated as payload inside another IP packet, some of the outer header fields can be newly written and others are determined by the inner header. Among these fields is the IP DF (Do not fragment) flag. When the inner packet DF flag is clear, the outer packet may copy it or set it. However, when the inner DF flag is set, the outer header MUST copy it.
Set DF Flag	If the DF (Do not Fragment) flag is set, it means the fragmentation of this packet at the IP level is not permitted.



XC-DPG503

Twin WAN VPN Gateway

Chapter Contents

- SNMP
- Email Alert
- Syslog
- Upgrade Firmware

Chapter 8 - Management Assistant

SNMP - Simple Network Management Protocol

This section is to compliment any SNMP (Simple Network Management Protocol) software installed on your PC. If you have SNMP software, you can use a standard MIB II file with the XC-DPG503.

Settings - SNMP

System Information

- **Contact Person** - The name of the person responsible for this device
- **Device Name** - Enter a name for the XC-DPG503
- **Physical Location** - The location of the XC-DPG503

Trap Targets

Enter the IP address of any targets (PCs running SNMP software) to which you want traps to be sent. All traps are level 1.

Email Alert

The email alert feature will send an warning email to the system administrator and inform that one of the WAN ports was disconnected.

Email Alert	<ul style="list-style-type: none"> • Enable – This will enable email alert to send an warning email when WAN port was disconnected. • Disable – This will disable email alert not to send an warning email when WAN port was disconnected.
Email Sender Address	<p>Email Sender Address An email address that sends a warning email to a recipient. The warning email will inform the recipient if there is any problem on either or both WAN ports.</p> <p>Email (SMTP) Server Address This sets the email server to where the warning email will be sent to. For example: <i>mail.domain.com</i>.</p> <p>Email (SMTP) server user name This authenticates the user name of email sender (optional).</p> <p>Email (SMTP) server password This is the user password</p>

Management Assistant

Email Alert (continued)

Email (SMTP) Server Address	This field sets the email sever's address for the warning email will be sent to. (<i>Email Alert must be enabled</i>) For example: <i>mail.domain.com</i>
Email Recipient Address	This field sets the email address for the warning email will be sent to. This is usually the system administrator email address. For example: <i>admin@mail.domain.com</i>
Excessive Ping Notification	This feature is useful to prevent ICMP attacks from WAN or LAN. It will drop the packets if the ping times are exceeding the threshold value. A notification email will be sent to the administrator.

Syslog

This feature can send real time system information on a web page or to a specified PC.

Syslog Configuration

Syslog Configuration allow you where to send system information to another machine or not. There are up to three machines you can choose to send your system log to.

Message Status

Messages send only keep when “*keep send message*” checked. The XC-DPG503 keeps last 100 messages in the RAM. These messages will clear when reboot or powered off.

Syslog Configuration

Syslog Global	Enable – This allows the XC-DPG503 to send system log messages to other PCs.
Keep Sent Messages	Enable – When enabled the XC-DPG503 will keep sent messages. If not enabled, sent messages will be deleted.
Syslog Server	<ul style="list-style-type: none">• IP address: Up to 3 syslog servers can be used.• Enable: You can enable or disable each server temporarily.• Port: If your syslog server does not use the default port, you can change it.• Log Priority Level: The syslog messages are divided into 8 levels, from Emergency to Debug level. The lower the level, the less messages will be generated. Emergency is the lowest priority level and Debug is the highest one.

Management Assistant

Admin Password Screen

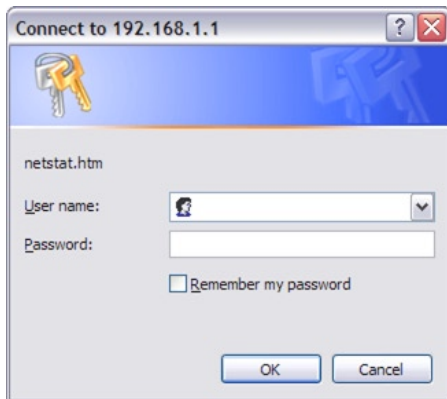
The password screen allows you to assign a password to the XC-DPG503.

Admin. Password

Administrator Password	
User Name	admin
Password	<input type="password"/>
Verify Password	<input type="password"/>

Enter the desired password. Re-enter the password in the Verify Password field and then save it.

When you connect to the XC-DPG503 with your Browser, you will be prompted for the password when you connect, as shown below.



- Enter "Admin" for the User Name.
- Enter the password for the XC-DPG503 as set on the Admin Password screen above.

Upgrade Firmware

Using the TFTP Utility (Recommended)

The XC-DPG503 Twin WAN Router supports the Trivial File Transfer Protocol (TFTP). This is mainly used to upload the firmware to the device. It can also be used to save and upload the configuration and reset the router to defaults. This guide will show you how to perform all those actions along with the proper procedure for upgrading your XC-DPG503 to the latest firmware release.

Updating the Firmware

To update the firmware on your XC-DPG503 you must first download the firmware from the XiNCOM Support web page (<http://www.xincom.com/support>) You will need an unzipping utility such as WinZip (www.winzip.com) or WinRAR (www.rarlab.com) to extract the contents of the file. Included will be a README file (usually README.txt), TFTP (tftp.exe) utility and the firmware file ({name}.bin).

Backup your configuration

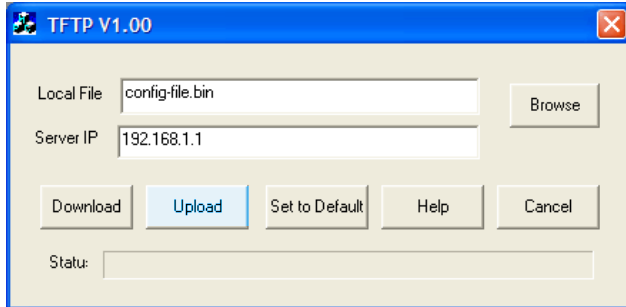
When you update the firmware on the XC-DPG503 the default configuration overwrites any settings that you previously entered into the router. You will need to save the configuration of the file to the router. There are two ways to do this, the TFTP utility and the HTTP user interface. This section covers only the TFTP utility, you can learn how to update using the HTTP utility in the Admin Control section.

To save the XC-DPG503 Configuration to a file:

1. Open the TFTP utility by double clicking on it.
2. Enter the routers IP address (Default is: 192.168.1.1)
3. Enter a file name that you would like to save the file as (Example: config-file.bin).
4. Press the Upload button and the file will be saved to the same directory as the TFTP utility.

Management Assistant

Example of how to configure to save file.



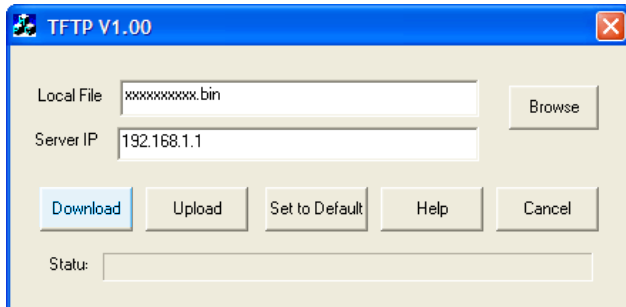
Uploading the Firmware

Using the TFTP utility you are able to update the firmware on the XC-DPG503, this is useful when you also need to recover the router from a crash.

To upload the firmware to the router:

1. Open the TFTP utility by double-clicking on it.
2. Enter the routers IP address (Default is: 192.168.1.1)
3. Click the Browse button and select the firmware file.
4. Click the Download button. It could take up to 1 to 3 minutes to upload the firmware, after which the router will reboot.

Example of how to configure to upload firmware.



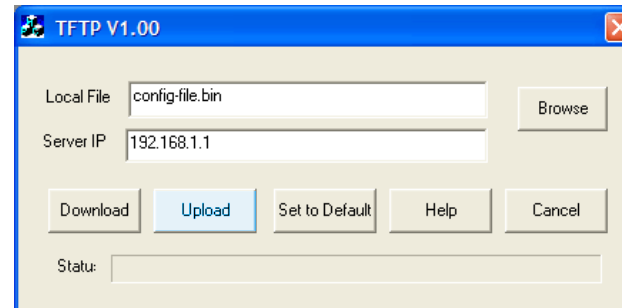
Restoring Saved Configuration

Once you have updated your firmware you are able to upload previously saved configuration.

To upload previously saved configuration:

1. Open the TFTP utility by double-clicking on it.
2. Enter the routers IP address (Default is: 192.168.1.1)
3. Click the Browse button and select the configuration file.
4. Click the Download button. It could take up to 1 to 3 minutes to upload the configuration, after which the router will reboot.

Example of how to configure to upload previously saved configuration.



HTTP Upgrade Firmware

The Upgrade Firmware Screen within the XC-DPG503's setup console allows you to upgrade firmware or backup system configuration by using HTTP upgrade.

- You can backup your system configuration by press "save" button of Save System Configuration. It will save the system configuration for you. (Notice: You have to refresh the browser after you saved the system configuration file)
- You also can do firmware upgrade by input the correct password and the file name of your firmware. Remember do not Reset or Restart the device while update new firmware, because it may cause system to crash.



XC-DPG503

Twin WAN VPN Gateway

Chapter Contents

- System Status
- Restore Factory Defaults
- WAN Status
- LAN Status

Chapter 9 - Operation & Status

Operation & Status Overview

Once both the XC-DPG503 and the PCs are configured, operation is automatic. However, there are some situations where additional Internet configuration may be required (*Refer to Chapter 4 - Advanced Features for further details*)

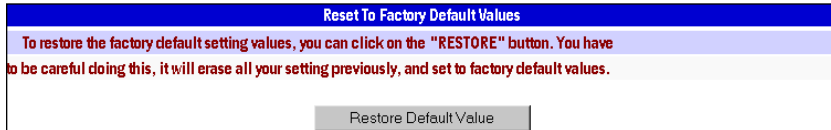
System Status

WAN Information	<p>Connection Status – Current status – either “Connected” or “Not connected”.</p> <p>Connection Type – The type of connection used – DHCP, Fixed IP, PPPoE, or PPTP.</p> <p>Force Renew button– Only available when using a dynamic IP address (DHCP). Clicking this button will perform a DHCP “Renew” transaction with the ISP’s DHCP server. This will extend the period for which the current WAN IP address is allocated to you.</p> <p>IP Address – The IP address of the XC-DPG503 when seen from the Internet. This IP Address is allocated by the ISP (Internet Service Provider).</p> <p>Subnet Mask – The Network Mask (Subnet Mask) for the IP Address above.</p> <p>Domain Name IP Address – The address of the current DNS (Domain Name Server).</p> <p>MAC Address – The MAC (physical) address of the XC-DPG503 when seen from the Internet.</p>
LAN Information	<p>IP Address – The LAN IP Address of the XC-DPG503.</p> <p>Subnet Mask – The Network Mask (Subnet Mask) for the IP Address above.</p> <p>MAC Address – The MAC (physical) address of the XC-DPG503 when seen from the local LAN.</p> <p>DHCP Server – The status of the DHCP Server function - either “Enabled” or “Disabled”.</p>
Device Information	<p>Firmware Version – Version of the Firmware currently installed.</p> <p>NAT – Status of the NAT feature – either “Enable” or “Disable”.</p> <p>Load Balance – Status of the Load Balance feature – either “Enable” or “Disable”.</p> <p>Virtual Server – Status of the Virtual Server feature – either “Enabled” or “Disabled”.</p> <p>Special Applications – Status of the Special Applications feature – either “Enabled” or “Disabled”.</p> <p>DMZ – Status of the DMZ feature – either “Enabled” or “Disabled”.</p> <p>Block URL – Status of the Block URL feature – either “Enable” or “Disable”.</p> <p>Hardware ID – The manufacturers ID for this particular device.</p>
Device Statistics	<p>System UpTime – The time since the system of a device was last re-initialized.</p> <p>CPU Usage – The current usage percentage of CPU.</p> <p>Memory Usage – The current usage percentage of Memory (Heap & Queue).</p>
Buttons	<p>Refresh – Update the data on screen.</p> <p>Restart – Restart (reboot) the XC-DPG503.</p> <p>Restore Factory Defaults – This will delete all existing settings, and restore the factory default settings.</p>

Operation & Status

Restore Factory Defaults

When the **“Restore Factory Defaults”** button on the **Status** screen above is clicked, the following screen is displayed.



If the **“Restore Default Value”** button on this screen is clicked:

- ALL of your settings will be erased.
- The default IP address, password and ALL other settings will be restored to the factory default values.
- The DHCP server function will be enabled.

These changes may mean that the current connection is invalid and you will have to re-connect to the XC-DPG503 using its default IP address (192.168.1.1).

WAN Status

NAT Statistics	<p>This section displays data for each WAN port.</p> <p>Connection status – This will display either Connected or Not Connected.</p> <p>Default Loading Share - The default traffic loading between the WAN ports.</p> <p>Current Loading Share – The current traffic loading between the WAN ports.</p> <p>Current Loading – The number of sessions, Bytes and Packets currently being processed on each port.</p> <p>Current Bandwidth – The current Download and Upload speeds on each WAN port.</p> <p><i>“Check NAT Detail”</i> will display the NAT Status screen, described below.</p>
Interface Statistics	<p>This section displays cumulative statistics.</p> <p>Use the <i>“Restart Counter”</i> button to restart these counters when required.</p>

NAT Status

LAN IP Info	<p>IP Address – The LAN IP Address of the XC-DPG503.</p> <p>Mask Address – The Network Mask (Subnet Mask) for the IP Address above.</p>
Active WAN IP Info	<p>There is one (1) row for each active connection. For each connection the following data is shown:</p> <p>IP Address – The WAN (Internet) IP Address of the XC-DPG503.</p> <p>Mask Address – The Network Mask (Subnet Mask) for the IP Address above</p>
NAT Timeouts	This displays the current timeout values for TCP and UDP connections.
TCP Prosperity	This displays the MSS (Maximum Segment Size) and Maximum Windows size for TCP packets.
NAT Traffic	This section displays statistics for both outgoing (LAN to Internet) and Incoming (Internet to Local) traffic.
NAT Connections	This displays the current number of active connections. For further details, click the <i>“View Connection”</i> list button.
Errors	Statistics are displayed for Checksum errors, number of retries, and number of bad packets.
Misc.	This displays the total IP packets and reserved address.



XC-DPG503

Twin WAN VPN Gateway

Chapter Contents

- Overview
- Existing DHCP Server
- Static Routing

Chapter 10 - Advanced LAN Configuration

Overview

These settings are provided to deal with non-standard situations or to provide additional options for advanced users.

Existing DHCP Server

If your LAN already has a DHCP Server, and you wish to continue using it, the following configuration is required.


- The DHCP Server function in the XC-DPG503 must be disabled. This setting is on the LAN & DHCP screen.
- Your DHCP Server must be configured to provide the XC-DPG503's LAN IP address as the "Default Gateway".
- Your DHCP Server must provide correct DNS addresses to the PCs.

Advanced LAN Configuration

Static Routing

This section is only relevant if your LAN has other Routers or Gateways.

- If you do not have other Routers or Gateways on your LAN, skip the Static Routing page.
- If your LAN has other Gateways and Routers, you must configure the Static Routing screen as described below. You also need to configure the other Routers.

Static Routing 

Static Routing Entry

Entry Index	<input type="text" value=""/> <input type="button" value="Select"/>
Network Address	<input type="text" value="0.0.0.0"/>
Netmask	<input type="text" value="0.0.0.0"/>
Gateway	<input type="text" value="0.0.0.0"/>
Interface	<input type="text" value="LAN"/>
Metric	<input type="text" value="0"/> (2~15)

Routing List

Index	Destination IP	Subnet Mask	Gateway	Interface	Metric	Type
0	192.168.9.1	255.255.255.255	192.168.9.1	WAN1	15	System
0	192.168.1.2	255.255.255.255	192.168.1.2	LAN	15	System
1	192.168.10.1	255.255.255.255	192.168.10.1	WAN2	2	Manual
0	192.168.9.7	255.255.255.255	192.168.9.7	WAN1	15	System

Note: If there is an entry or entries in the Routing table with an Index of zero (0), these are System entries. You can not modify or delete these entries.

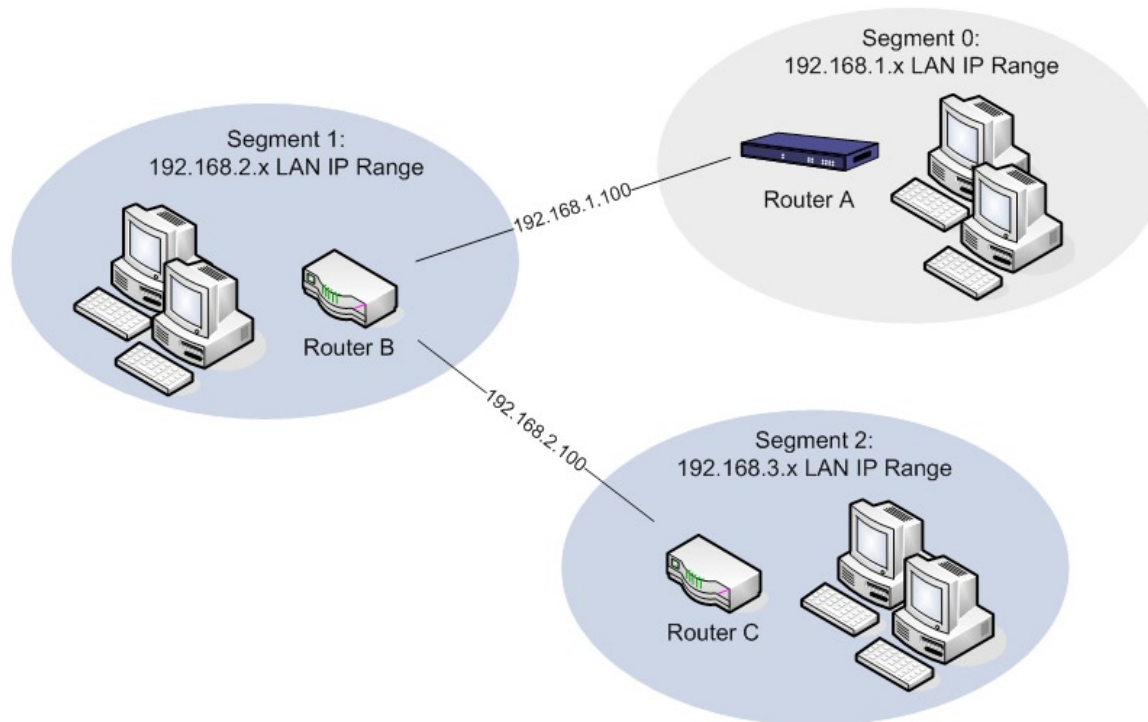
Settings - Static Routing

Entry Index	<ul style="list-style-type: none">• If adding a new entry, skip this field.• To edit an existing entry, select it from the list, and click the "Select" button. The screen will then update with the data for the selected entry.• If the Index is 0, this is a System entry which you can neither delete nor modify.
Network Address	The network address of the remote LAN segment. For standard class "C" LANs, the network address is the first 3 fields of the Destination IP Address. The 4th (last) field can be left at 0.
Netmask	The Network Mask for the remote LAN segment. For class "C" networks, the default mask is 255.255.255.0
Gateway	The IP Address of the Gateway or Router which the XC-DPG503 must use to communicate with the destination above. (NOT the router attached to the remote segment.)
Interface	Select the correct interface (usually LAN). The WAN interface is only available if NAT (Network Address Translation) is disabled.
Metric	The number of "hops" (routers) to pass through to reach the remote LAN segment. The shortest path will be used.

Advanced LAN Configuration

Configuring other Routers on your LAN

All traffic for devices not on the local LAN must be forwarded to the XC-DPG503 so that they can be forwarded to the Internet. This is done by configuring other Routers to use the XC-DPG503 as the Default Route or Default Gateway, as illustrated by the example below:



Configuration settings for the LAN shown with 2 routers and 3 LAN segments, the XC-DPG503 requires 2 entries as follows.

For the XC-DPG503 Gateway's Routing Table

Entry 1 (Segment 1)	
Destination IP Address	192.168.2.0
Network Mask	255.255.255.0
Gateway IP Address	192.168.1.100
Interface	LAN
Metric	2
Entry 2 (Segment 2)	
Destination IP Address	192.168.3.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.1.100
Interface	LAN
Metric	3

For Router A's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.1.1
Metric	2

For Router B's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.2.80
Interface	LAN
Metric	3



XC-DPG503

Twin WAN VPN Gateway

Chapter Contents

- Appendix A - Specifications
- Appendix B - Windows TCP/IP Setup
- Appendix C - Troubleshooting

Appendices

Appendix A Specifications

Model	XC-DPG503
Dimensions	245mm (W) x 137mm (D) x 30mm (H)
Operating Temperature	0° C to 40° C
Storage Temperature	-10° C to 70° C
Network Protocol	TCP/IP
Network Interface	6 Ethernet: 4 x 10/100BaseT (RJ45) auto-Switching Hub ports for LAN devices 2 x 10/100BaseT (RJ45) for WAN
LEDs	8 LAN 4 WAN 1 Status 1 Power
External Power Adapter	5 V 1.5A DC

FCC Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference.
- (2) This device must accept any interference received, including interference that may cause undesired operation.

CE Marking Warning

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Appendices

Appendix B

Windows TCP/IP Setup

TCP/IP Settings

If using the default XC-DPG503 settings, and the default Windows 95/98/ME/2000 TCP/IP settings, no changes need to be made.

- By default, the XC-DPG503 will act as a DHCP Server and automatically provide a suitable IP Address (and related information) to each PC when the PC boots.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client.
- If you wish to check your TCP/IP settings, the procedure is described in the following sections.
- If your LAN has a Router, the LAN Administrator must re-configure the Router itself. Refer to Chapter 5 – Advanced LAN Setup for details.

Checking TCP/IP Settings - Windows 9x/ME

1. Select *Control Panel - Network*. You should see a screen like the following:

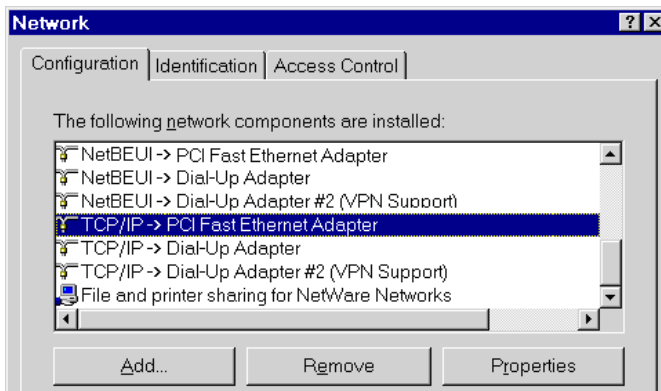


Figure A. Network Configuration

2. Select the TCP/IP protocol for your network card.
3. Click on the Properties button. You should then see a screen as showed in Figure B.

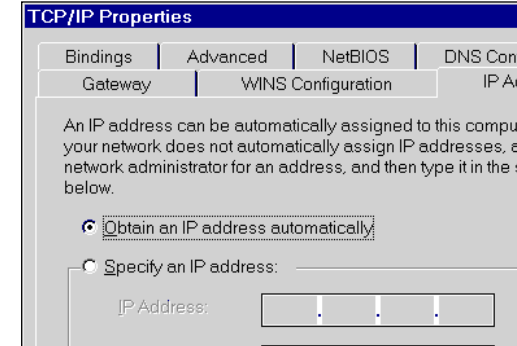


Figure B. IP Address (Windows 95)

Ensure your TCP/IP settings are correct, as follows:

Using DHCP

To use DHCP, select the radio button Obtain an IP Address automatically. This is the default Windows settings.

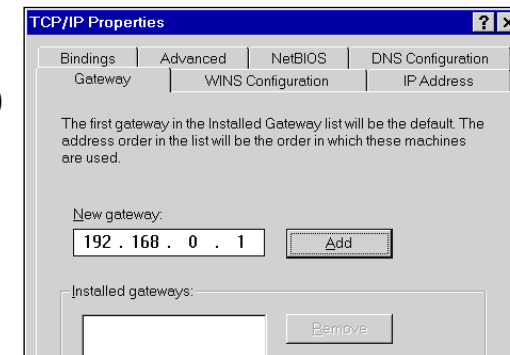
Restart your PC to ensure it obtains an IP Address from the Link Balancer.

Using “Specify an IP Address”

If your PC is already configured, check with your network administrator before making the following changes:

- If the DNS Server fields are empty, select Use the following DNS server addresses, and enter the DNS address or addresses provided by your ISP, then click OK.
- On the Gateway tab, enter the IP address of the XC-DPG503 in the New Gateway field and click Add, as shown below. (Your LAN administrator can advise you of the IP Address they assigned to the XC-DPG503)

Figure C. Gateway Tab (Windows 95/98)



Appendices

- On the *DNS Configuration* tab, ensure *Enable DNS* is selected. If the *DNS Server Search Order* list is empty, enter the DNS address provided by your ISP in the fields beside the *Add* button, then click *Add*.

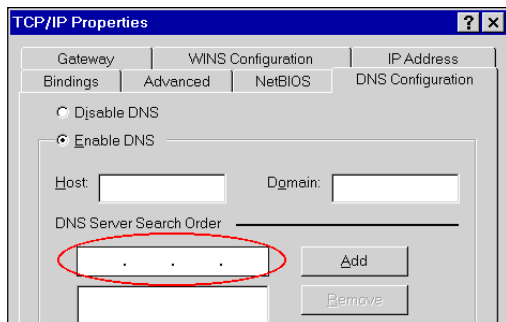


Figure D. DNS Tab (Windows 95/98)

Checking TCP/IP Settings - Windows 2000:

1. Select *Control Panel - Network and Dial-up Connection*.
2. Right click the *Local Area Connection* icon and select *Properties*. You should see a screen like the following:

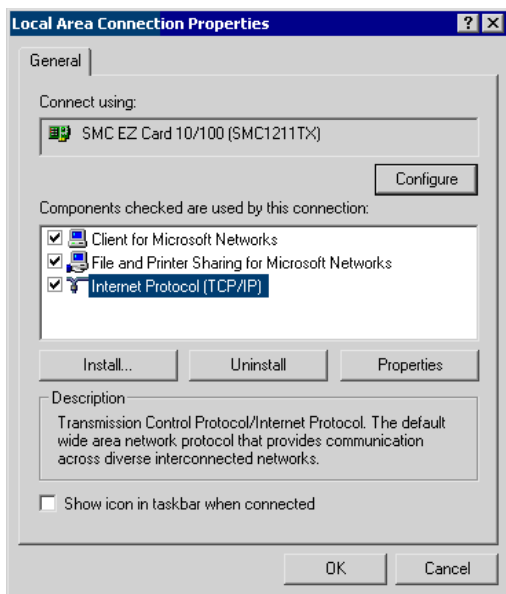


Figure E. Network Configuration (Windows 2000)

3. Select the TCP/IP protocol for your network card.
4. Click on the Properties button. You should then see a screen like the following.

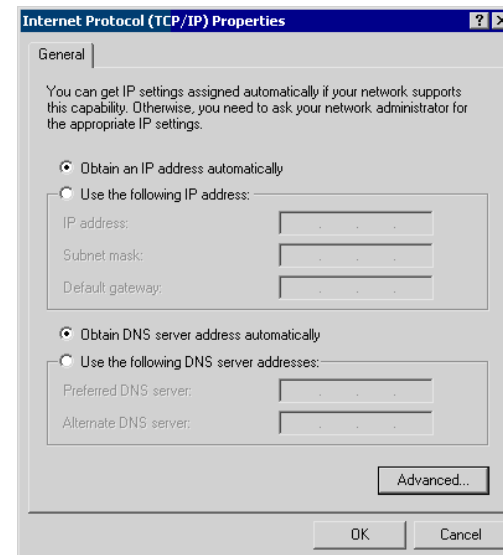


Figure F. TCP/IP Properties (Windows 2000)

5. Ensure your TCP/IP settings are correct:

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows settings.

Restart your PC to ensure it obtains an IP Address from the XC-DPG503.

Using a fixed IP Address (“Use the following IP Address”)

If your PC is already configured, check with your network administrator before making the following changes:

- Enter the IP address of the XC-DPG503 in the *Default gateway* field and click OK. (Your LAN administrator can advise you of the IP Address they assigned to the XC-DPG503)
- If the DNS Server fields are empty, select *Use the following DNS server addresses*. Enter the DNS address or addresses provided by your ISP and then click OK.

Appendices

Checking TCP/IP Settings - Windows XP:

1. Select Control Panel - Network Connection.
2. Right click the *Local Area Connection* and choose *Properties*.
You should see a screen like the following:

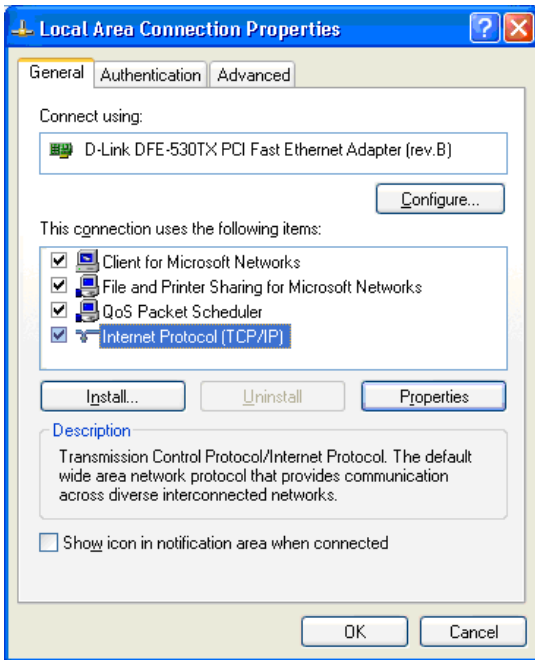


Figure G. Network Configuration (Windows XP)

3. Select the TCP/IP protocol for your network card.

4. Click on the *Properties* button. You should then see a screen like the following:

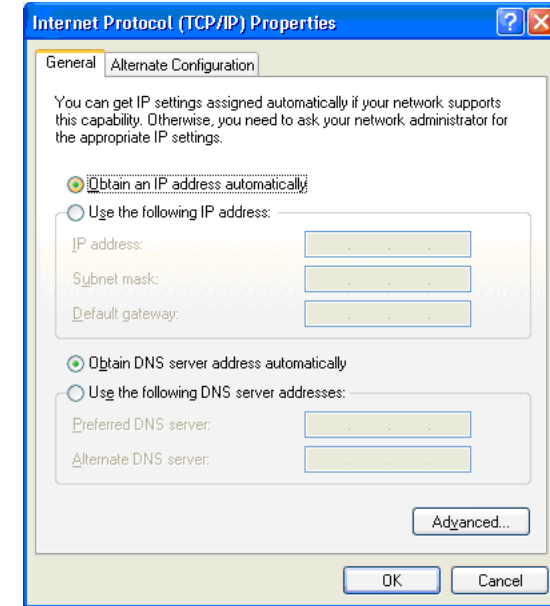


Figure H. TCP/IP properties (Windows XP)

5. Ensure your TCP/IP settings are correct.

Using DHCP

To use DHCP, select the radio button *obtain an IP Address automatically*. This is the default Windows settings.

Restart your PC to ensure it obtains an IP Address from the XC-DPG503.

Using a fixed IP Address (“Use the following IP Address”)

If your PC is already configured, check with your network administrator before making the following changes.

- Enter the IP address of the XC-DPG503 in the *Default gateway* field and click OK. (Your LAN administrator can advise you of the IP Address they assigned to the XC-DPG503)
- If the DNS Server fields are empty, select *Use the following DNS server addresses*. Enter the DNS address or addresses provided by your ISP and then click OK.

Appendices

Appendix C

Troubleshooting

Overview

This chapter covers some common problems that may be encountered while using the XC-DPG503 and some possible solutions to them. If you follow the suggested steps and the XC-DPG503 still does not function properly, contact XINCOM for further advice.

General Problems

Problem:	I can't connect to the XC-DPG503 to configure it.
Solution:	<p>Check the following:</p> <ul style="list-style-type: none">○ The XC-DPG503 is properly installed, LAN connections are OK, and the device is powered ON.○ Ensure that your PC and the XC-DPG503 are on the same network segment.○ If your PC is set to <i>Obtain an IP Address automatically</i> (DHCP client), restart it.○ If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 192.168.1.2 to 192.168.1.254 and thus compatible with the XC-DPG503's default IP Address of 192.168.1.1.○ Also, the Network Mask should be set to 255.255.255.0 to match the XC-DPG503.○ In Windows, you can check these settings by using <i>Control Panel-Network</i> to check the <i>Properties</i> for the TCP/IP protocol.

Internet Access

Problem 1:	When I enter a URL or IP address I get a time out error.
Solution 1:	<p>A number of things could be causing this. Try the following troubleshooting steps:</p> <p>Check if other PCs work. If they do, ensure that your PCs IP settings are correct. If using a Fixed (Static) IP Address, check the Network Mask, Default gateway and DNS as well as the IP Address.</p> <p>If the PCs are configured correctly, but still not working, check the XC-DPG503. Ensure that it is connected and ON. Connect to it and check its settings. (If you cannot connect to it, check the LAN and power connections.)</p> <p>If the XC-DPG503 is configured correctly, check your Internet connection (DSL/Cable modem etc) to see that it is working correctly.</p>
Problem 2:	Some applications do not run properly when using the XC-DPG503.
Solution 2:	<p>The XC-DPG503 processes the data that passes through it and therefore it does not act as a transparent device.</p> <ul style="list-style-type: none">○ Use the Special Applications feature to allow the use of Internet applications which do not function correctly.○ If this does solve the problem you can use the DMZ function. This should work with most applications, but:<ul style="list-style-type: none">• It is a security risk, since the firewall is disabled for the DMZ PC.• Only one (1) PC can use this feature.